OCT 31 1987

GA1.13:PEMD-86-5

United States General Accounting Office

GAO

Report to the Chairman, Committee on
Governmental Affairs
United States Senate

COMPLETED
129

April 1986

TECHNICAL RISK ASSESSMENT

The Status of Current DOD Efforts

GAO/PEMD-86-5

GAO

United States
General Accounting Office
Washington, D.C. 20548

Comptroller General
of the United States

B-221769

April 3, 1986

The Honorable William V. Roth, Jr.
Chairman, Committee on Governmental Affairs
United States Senate

Dear Mr. Chairman:

This report responds to your February 26, 1985, letter asking the General Accounting Office to evaluate policies and procedures for technical risk assessment in the Department of Defense. In the report, we make six recommendations, covering basic risk assessment concepts, policy, and operational procedures. Each recommendation is directed to the Secretary of Defense.

Officials of DOD were asked to comment on the draft of the report. Their comments appear with our answers in appendix III. DOD generally concurred with our findings and recommendations, but we believe it is critical to monitor DOD's further efforts. For example, the new risk assessment handbook to be prepared by the Defense Systems Management College should cover the assessment of technical risk, not just the management of program risk in general. Coming hearings on DOD management will present an opportunity for the further review of technical risk assessment in DOD and for the direct expression of continuing congressional interest in this subject.

As we agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of the report. At that time, we will send copies to those who are interested and will make copies available to others upon request.

Sincerely yours,

Charles A. Bowsher

Charles A. Bowsher
Comptroller General
of the United States

Executive Summary

Technical risks are inherent in the development of new weapon systems whose performance requirements exceed the capabilities of current weapon systems. If not anticipated and managed early in the acquisition process, these risks can have profound effects on a program's cost and schedule and, ultimately, the effectiveness of the armed forces.

The Department of Defense (DOD) has identified technical problems as a major factor in cost growth and schedule delays and has reported that the level of technical risk directly affects decisions on further development. In 1981, DOD called for a greater use of quantitative risk assessments to support the budgeting of extra funds to cover technical risk. By 1983, DOD informed the Congress that the services had implemented this initiative.

Despite the critical value of technical risk assessment and its reported prominence in DOD's acquisition decisions, very little is known about either its characteristics or the information on risk that is made available to program managers and reviewers.

The Senate Governmental Affairs Committee asked GAO to examine current DOD policies and practices governing the assessment of technical risk and report on the quality and availability of DOD's technical risk information.

Background

Technical risk assessment for a weapon system being developed is the responsibility of the system's program management office. The purposes of assessment generally include identifying technical problems that may occur, rating the likelihood of their occurrence, and estimating the extra funds needed to solve them. The results are to be used to guide technical decisions and program scheduling and budgeting.

To examine current DOD policies and practices, GAO obtained relevant documents, interviewed representatives of DOD and the services, and analyzed risk-related efforts in 25 program offices covering all major weapon systems relevant to GAO's purposes. In December 1984, development and production costs of these systems together were estimated to exceed $180 billion.

Results in Brief

Despite DOD's concern with technical risk and its potential effect on defense, DOD has no clear definition of technical risk and has not developed advice or training sufficient to guide the selection and implementation of various analytical approaches (pp. 24-33, 54-62, and 68-69).

In most of the 25 program offices GAO reviewed, the design and implementation of efforts to assess technical risk have not met minimal standards of quality. Essential information on assessment procedures and results has often not been available to program managers or reviewers (pp. 33-51 and 62-71).

Principal Findings

Risk Assessment Guidance

DOD has identified many technical risk approaches, both quantitative and qualitative. But there is insufficient policy and training to guide program managers in the selection of suitable approaches. Further, no standard definition of technical risk exists within DOD. Accordingly, many program offices have developed their own informal definitions of technical risk and risk-rating categories, but GAO found them inconsistent and sometimes contradictory. Despite DOD's 1981 initiative, none of the 25 program offices had conducted a quantitative technical risk assessment to support budgeting for risk (pp. 24-33, 35, 54-62, and 68-69).

Design Criteria

Because DOD had not developed standards for its assessments, GAO derived criteria from management principles and previous research on risk. These are prospective assessment, planned procedures, documentation, explicit attention to technical risk, and reassessment in each acquisition phase. All 25 program offices had made some effort to identify their technical risks, but only 3 efforts met these criteria. The remaining 22 addressed risk in some way but did not fulfill one or more of the criteria (pp. 35-43).

Implementation

Turning from design to implementation, GAO found that few of the 25 program offices' risk efforts were carried out in ways likely to produce the most accurate and useful results. In this regard, 4 program offices had provided a description of technical problems and a rating of risk levels, 10 had covered all of a system's components, and 5 had collected data from independent raters (pp. 43-48).

Communication of Risk Information

Technical risk information was not always adequately conveyed to decisionmakers. Some program staff were unaware of the risk efforts carried out for their systems and others lacked important information on the assessment procedures and results. The documents and briefings GAO reviewed did not adequately describe assessment procedures or results. Further, when program offices received technical risk information from contractors, it was often not well documented (pp. 48-51 and 62-71).

Focus of GAO Review

Focusing on technical risk assessment processes, GAO made no attempt to appraise the accuracy of any assessment or to measure its effects. But findings indicate that the processes of risk assessment must be improved before its accuracy or outcomes can be successfully studied.

Recommendations to the Secretary of Defense

To reinforce DOD's emphasis on technical risk assessment, GAO recommends that the secretary of Defense

- define technical risk and categories for rating risk;
- require that risk efforts focus explicitly on technical risk and be prospective, planned, and repeated at least twice, early and late, in each acquisition phase;
- require program offices to document their risk assessment procedures and results;
- establish guidelines regarding options for format for rating risks, scope, data collection, and assessment approaches;
- require that the technical risk information that program offices or contractors provide for review include a description of format, scope, data collection, sources of risk information, and assessment approaches; and
- provide more focused training in technical risk assessment.

Agency Comments

DOD generally concurred with the principal findings but argued that the report overemphasizes technical problems as distinct from the cost and schedule components of overall program risk. DOD concurred fully or partially with all recommendations except the one calling for making additional information on risk assessment procedures available for review (GAO's fifth recommendation). DOD prefers more flexibility regarding the content of information that is provided for reviewers of assessment results and procedures. DOD also expressed reluctance to place further requirements on program management and argued that cost growth has declined to about 1 percent, rendering such requirements unnecessary (pp. 113-21).

GAO believes that the findings demonstrate a need for more clarity in, and attention to, technical risk assessment in DOD. The findings do not suggest that technical risk is more critical than cost or schedule risk or that DOD's attention to cost or schedule risk can be reduced. GAO believes greater consistency in assessment concepts and procedures is required but also recognizes the need for tailoring assessments to particular programs. GAO did not examine effects, but since most of DOD's assessments have not met minimal standards of quality, it is unlikely that they have contributed to any reductions in cost growth.

Contents

Executive Summary 2

Chapter 1 Introduction 10
DOD's Acquisition Process 11
Technical Risk Assessment 14
Objectives, Scope, and Methodology 15
Our Study's Strengths and Limitations 21

Chapter 2 DOD's Policies for Technical Risk Assessment 24
How Does DOD Define Technical Risk? 25
What Guidance Does DOD Provide for Assessing Technical Risk? 27
How Have the Services Implemented Initiative 11? 31
Summary 33

Chapter 3 Differences in How the Program Offices Address Technical Risk 34
What Are the Characteristics of Current Efforts to Identify the Technical Risks of New Systems? 35
How Are Efforts to Identify Technical Risk Implemented? 43
What Information on Technical Risk Is Available to Decisionmakers in the Review Process? 48
Summary 51

Chapter 4 Difficulties with Current Approaches to the Assessment of Technical Risk 54
Definitions of Risk and Risk Rating Categories 54
The Communication of Information to Decisionmakers 62
Program Management Office Staffing and Training 67
Reliance on Prime Contractors 69
Summary 71

Chapter 5 Conclusions and Recommendations 74
Conclusions 74
Recommendations to the Secretary of Defense 77
Agency Comments and Our Response 78

Appendixes

Appendix I: Program Descriptions 80
Appendix II: Bibliography 99

Appendix III: Advance Comments from the U.S. Department of Defense 113

Tables

Table 1.1: The 25 Major Systems We Examined and Their Milestone Review Status on September 15, 1984 18
Table 1.2: The Primary Data Sources for Our Evaluation Questions 19
Table 3.1: DOD Risk Efforts Rated on the Technical Risk Assessment Criteria 37
Table 3.2: Technical Risk Rating Scale for Remotely Piloted Vehicle 42
Table 3.3: Decisions and Options in the Implementation of Risk Efforts 44
Table 3.4: The Sources and Types of Information on Technical Risk at Milestones I and II 49
Table 3.5: The Format and Scope of Risk Ratings in Milestone Documents and Briefing Charts 51
Table 4.1: The Definitions of Technical Risk Used in the Program Management Offices 55
Table 4.2: Qualitative Risk Ratings in Narrative Terms Used in the Program Management Offices 57
Table 4.3: Advantages and Disadvantages of Quantitative Risk Efforts Cited by the Program Management Offices 60
Table 4.4: Advantages and Disadvantages of Qualitative Risk Efforts Cited by the Program Management Offices 61

Figures

Figure 1.1: DOD's Weapon System Acquisition Cycle 12
Figure 3.1: The Criterion of Reassessment in Each Acquisition Phase 40

Abbreviations

AHIP	Advanced Helicopter Improvement Program
ALWT	Advanced Lightweight Torpedo
AMRAAM	Advanced Medium-Range Air-to-Air Missile
ASAT	Antisatellite Weapon
ASPJ	Airborne Self-Protection Jammer
ASW SOW	Antisubmarine Warfare Standoff Weapon
ATRS	Advanced Tactical Radar System
C-17A	C-17A Airlift Aircraft System
CV-HELO	CV Innerzone Antisubmarine Warfare Helicopter
DOD	U.S. Department of Defense
DSARC	Defense Systems Acquisition Review Council
GAO	U.S. General Accounting Office
HFAJ	High Frequency Anti-Jammer
I-S/A AMPE	Inter-Service/Agency Automated Message Processing Exchange
JSTARS	Joint Surveillance and Target Attack Radar System
JTIDS	Joint Tactical Information Distribution System
Mark XV IFF	Mark XV Identification Friend or Foe
MLRS/TGW	Multiple Launch Rocket System Terminal Guidance Warhead
MMS	Mast-mounted sight
M1A1	M1 Abrams Tank Enhancement
NAVSTAR User Equipment	NAVSTAR Global Positioning System User Equipment
RDT&E	Research, development, test, and evaluation
RPV	Remotely Piloted Vehicle
SARC	Systems Acquisition Review Council
SHORAD C2	Short-Range Air Defense Command and Control System
SRAM II	Short-Range Attack Missile II
SUBACS	Submarine Advanced Combat System
T45TS	T-45 Training System
TRACE	Total risk assessing cost estimate
Trident II (D5)	Trident II D5 Weapon System

BLANK PAGE

Chapter 1

Introduction

Technical risks are inherent in the development of new weapon systems, whose advanced performance requirements may exceed the capabilities of current technology. Not to anticipate technical risks before and during the development process creates the potential for scheduling and cost problems and, worse, the possibility that a system will fail to meet its design specifications and will not function as intended. In line with this, a 1983 Air Force report on an "affordable acquisition approach" found technical problems a factor in more than 50 percent of the programs that experienced cost growth.

It is understandable that technical problems may occur in the development of systems that must achieve performance goals beyond any yet attained, as for example with the need for significant improvements in the accuracy of the submarine-launched Trident II missile over the Trident I. But it is important to recognize that technical problems may occur in time to plan and budget for solving them and to specify possible alternative technical approaches. Technical risk assessment is the process for identifying and evaluating the potential for performance problems.

Recognizing the hazards of not anticipating technical risks, the Department of Defense (DOD) has focused on the need to identify and plan for technical risk in defense production in various ways:

1. As early as 1969, the deputy secretary of Defense directed the secretaries of the armed services to identify areas of high technical risk, do formal risk analysis, and include explicit consideration of risk assessment, reduction, and avoidance in managing weapon systems acquisition.

2. In 1981, the deputy secretary of Defense recommended that each service expand its efforts to quantify the technical risks of systems being developed and to allocate funds to deal with these risks. (This recommendation, known as Initiative 11, is discussed in chapter 2.)

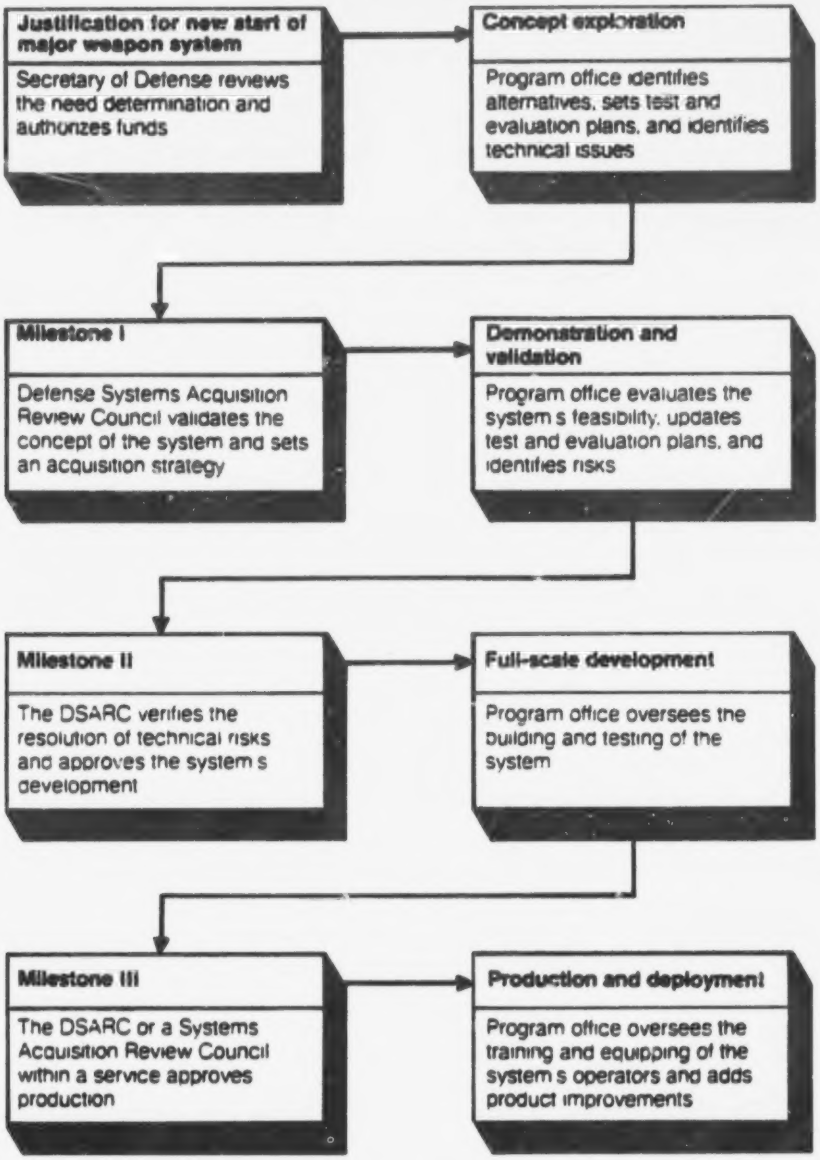
3. In recent testimony before the Congress, Defense officials stated that funding would be approved for systems with only low or moderate technical risk. But identifying such systems poses problems, since DOD has stated that ratings of risk are subjective and that it is necessary to be cautious in categorizing risks as high, moderate, or low.

DOD's Acquisition Process

The DOD acquisition process is complex, yet some familiarity with the phases of development and major decision points is necessary in order to understand the issues involved in technical risk assessment, because attention to technical risks is required in these phases. At each decision point, there are several levels of review, culminating with the Defense Systems Acquisition Review Council (DSARC) or, if delegated by the DSARC, a Systems Acquisition Review Council (SARC) within the appropriate service. The DSARC provides advisory support to the secretary of Defense, who is the deciding authority.

For each major weapon, there are four phases of acquisition, the first three of which end with a "milestone" decision by the DSARC or delegated to the service SARC. The phases are concept exploration, demonstration and validation, full-scale development, and production and deployment. These phases and their relevance to technical issues are described below and summarized in figure 1.1.

Figure 1.1: DOD's Weapon System Acquisition Cycle



Justification for new start of major weapon system

Secretary of Defense reviews the need determination and authorizes funds

Concept exploration

Program office identifies alternatives, sets test and evaluation plans, and identifies technical issues

Milestone I

Defense Systems Acquisition Review Council validates the concept of the system and sets an acquisition strategy

Demonstration and validation

Program office evaluates the system's feasibility, updates test and evaluation plans, and identifies risks

Milestone II

The DSARC verifies the resolution of technical risks and approves the system's development

Full-scale development

Program office oversees the building and testing of the system

Milestone III

The DSARC or a Systems Acquisition Review Council within a service approves production

Production and deployment

Program office oversees the training and equipping of the system's operators and adds product improvements

Concept Exploration

Justification for initiating development of a new system is provided by a "need determination," which is part of DOD's planning, programming, and budgeting system and is normally submitted when funds for the program objectives memorandum budget year are requested. One consideration in establishing need is technological advancement. The secretary provides program guidance after the memorandum review, thus officially sanctioning the start of the new program and authorizing acquisition to begin when funds are available.

A program management office then acquires information necessary to select the best alternatives for system concepts and the development of hardware and software. It also establishes the technical specifications and economic basis for the proposed system and develops a statement of the objectives, responsibilities, resources, and schedule for all test and evaluation efforts. One program responsibility in this phase is to identify critical technical issues for subsequent resolution, in an effort to minimize future problems.

At milestone I, the requirement for the program is reviewed and validated, the validation being based upon this preliminary evaluation of the system concepts, cost, schedule, readiness objectives, and affordability. The milestone I decision establishes thresholds and objectives to be met and reviewed at milestone II, the acquisition strategy (including the nature and timing of the next decision point), and a not-to-be-exceeded dollar threshold that will carry the program through milestone II.

Demonstration and Validation

During this phase, the program management office accomplishes a variety of tasks relevant to the technical issues. It verifies preliminary design and engineering, analyzes trade-off proposals, prepares a formal requirement document, and validates the concept for the next phase, full-scale development. Prototypes are often used to demonstrate the feasibility of the system, subsystem, or components, system-specific test and diagnostic equipment, and support equipment. Plans for testing and evaluating the system are updated. The program office also ensures that the risks have been identified and are acceptable and that realistic fall-back alternatives have been established. Performance estimates are reviewed for consistency with the risks involved.

This phase ends with milestone II, approval to go ahead with the program. The timing of the decision is flexible, depending on the acquisition strategy adopted at milestone I. At milestone II, all significant risk areas are resolved, so that the technology is in hand and only engineering (rather than experimental) efforts remain.

Full-Scale Development

In the development phase, the system, including training devices, computer resources, and other items necessary for its support, is fully developed, engineered, fabricated, and tested. Milestone III, the decision to proceed with the production of a major weapon system, is normally delegated by the secretary of Defense to the service secretary, unless thresholds established at milestone II were breached or the public or the Congress is greatly concerned about, for example, persistent technical problems or cost growth.

Production and Deployment

During the final phase, the service trains operational units, produces and distributes equipment, and provides logistical support. Product improvements, as required, are introduced.

Exemptions from the Acquisition Phases

A major weapon system may be granted exemptions from some phases of the full process. For example, a system that is judged not to require a full concept exploration, as may happen with a follow-on to an existing system, may skip to the demonstration and validation phase or combine concept exploration with demonstration and validation into a single effort prior to full-scale development. Milestone reviews may also be skipped or delayed if there are no distinct concept exploration and demonstration and validation phases or if the program has been restructured.

Technical Risk Assessment

As a system moves through the acquisition cycle, the program office is responsible for identifying, monitoring, and solving its technical problems. At each milestone, reviewers are to appraise the sources of risk and the progress of the program office in reducing risk. According to DOD policy, these efforts are to be based on the technical risk assessment for the system.

Assessment has many possible approaches. Usually, one or more technical experts identify particular components of the system being developed and then describe or rate the risk associated with each component. Their ratings may reflect the level of risk and sometimes also reflect the consequences of possible technical problems for the cost, schedule, or performance of the overall system. Ratings can be expressed in several formats—examples are a three-point scale ranging from high to moderate to low risk and a probabilistic estimate of the chance that technical problems will occur. The ratings can, in turn, be based on various sources of information, such as expert judgment, test or simulation results, and published technical reports on similar systems. Finally, some assessments cover only technical risk, while others cover technical along with cost and schedule problems or estimate the implications of technical problems for overall program cost and schedule. (Each of these components of program risk—technical, cost, and schedule risk—is critical, and each merits careful assessment.)

Chapter 2 provides detailed examples of various assessment approaches. Chapter 3 identifies criteria for appraising the quality of risk assessments and describes the methods DOD currently uses to manage the development of new systems.

Objectives, Scope, and Methodology

Recognizing that failure to adequately assess the technical risks for programs can result in excessive changes in design, prolonged delays, and substantial cost overruns, the Senate Governmental Affairs Committee asked us to examine DOD's policies governing technical risk and to review the quality of DOD's current assessment procedures and applications.

The Questions We Answered

To describe DOD's efforts to identify technical risks in the development of new systems, we formulated six evaluation questions covering assessment policies and practices across the three services.

1. How does the Department of Defense define technical risk? In addition to determining how DOD and the armed services define technical risk, we looked for differences in definition or ambiguities in meaning that might affect the way assessments are performed.

2. What guidance does DOD provide for assessing technical risk? Because defense system development is unique, we wanted to learn what assessment approaches, if any, DOD has developed or promoted for the use of the program management offices.

3. How have the services implemented Initiative 11? We sought to determine whether specific policies on technical risk assessment have resulted from Initiative 11, the 1981 DOD recommendation to the services for quantifying and budgeting for technical risk. We also sought to

examine differences in the way the services approach technical risk assessment.

4. What are the characteristics of current efforts to identify the technical risks of new systems? This question, aimed at describing efforts to identify technical risks for systems now under development, encompassed the largest set of issues. It included, for example, determining when these efforts are performed and whether they are being documented.

5. How are efforts to identify technical risks implemented? We sought to learn what formats are used to rate risk, whether the ratings cover specific subsystems or only a system as a whole, and how data on technical risk are collected.

6. What information on technical risk is available to decisionmakers in the review process? This question completed our examination of the acquisition process and, together with the five other evaluation questions, provided a framework for examining DOD's technical risk assessment policies, procedures, and applications.

The Risk Assessments We Examined

To answer the evaluation questions, we collected information from the Office of the Secretary of Defense, service headquarters staff, schools, laboratories, and defense contractors. Our principal data collection effort was gathering extensive information on technical risk assessments from 25 program offices managing the development of new systems. To obtain a full understanding of technical risk assessment throughout DOD, we examined all three services (the Army, Navy, and Air Force) and the differences between them.

We defined our universe of systems as all "major acquisitions" going through DSARC review. Major acquisitions are more costly, pose greater risks in development, and are more intensively reviewed by the secretary and the Congress than other acquisitions. Therefore, we saw them as the most likely to have had acquisition improvement initiatives and many related program management functions implemented. We excluded from our study some of the 43 major acquisitions that were under development on July 31, 1984, for three reasons.

1. Programs very early in the acquisition cycle lacked the documentation we needed and had not progressed through the review process. Programs very late in the cycle, those already in production, had already

passed through the review process, in which it had been certified that all technical risks had been resolved. In other words, we excluded programs that had not yet passed milestone I and those that had already passed milestone III. The programs we examined were in either the demonstration and validation phase or full-scale development.

2. We excluded ship hull programs (but not ship systems such as electronics) because of the long periods of time (up to 10 years) it takes to build them and the generally low level of technical risk associated with them.

3. Because of DOD's administrative decisions, we excluded the Army's guided antimortar projectile: DOD cancelled the program before we were able to collect data from the program management office. And we excluded the Navy's tactical microwave landing system, which DOD included among its major acquisitions to ensure that the secretary would review one of the system's components but exempted from DSARC milestone reviews (and, hence, it fell outside our parameters).

This left 25 systems in our universe, including 5 Army, 11 Navy, and 9 Air Force systems. (We classified joint-service programs according to the service with lead responsibility for development.) In December 1984, the projected development and production costs of these programs exceeded $180 billion. They are described briefly in appendix I and listed with their stages of development in table 1.1.

Table 1.1: The 25 Major Systems We Examined and Their Milestone Review Status on September 15, 1984

System	Abbreviation	Service
Between milestones I and II		
Antisubmarine Warfare Standoff Weapon	ASW SOW	Navy
Advanced Tactical Radar System	ATRS	Navy
C-17A Airlift Aircraft System	C-17A	Air Force
CV Innerzone Antisubmarine Warfare Helicopter	CV-HELO	Navy
High Frequency Anti-Jammer	HFAJ	Navy
Inter-Service/Agency Automated Message Processing Exchange	I-S/A AMPE	Air Force
Joint Surveillance and Target Attack Radar System	JSTARS	Air Force
Mark XV Identification Friend or Foe	Mark XV IFF	Air Force
Multiple Launch Rocket System/Terminal Guidance Warhead	MLRS/TGW	Army
Short-Range Air Defense Command and Control System	SHORAD C2	Army
Short-Range Attack Missile II	SRAM II	Air Force
T-45 Training System	T45TS	Navy
V-22 Osprey	V-22 Osprey	Navy
Between milestones II and III		
Army Helicopter Improvement Program	AHIP	Army
Advanced Lightweight Torpedo	ALWT	Navy
Advanced Medium-Range Air-to-Air Missile	AMRAAM	Air Force
Antisatellite Weapon	ASAT	Air Force
Airborne Self-Protection Jammer	ASPJ	Navy
Joint Tactical Information Distribution System	JTIDS (Air Force)	Air Force
Joint Tactical Information Distribution System	JTIDS (Navy)	Navy
M1 Abrams Tank Enhancement	M1A1	Army
NAVSTAR Global Positioning System User Equipment	NAVSTAR User Equipment	Air Force
Remotely Piloted Vehicle	RPV	Army
Submarine Advanced Combat System	SUBACS	Navy
Trident II D5 Weapon System	Trident II (D5)	Navy

The Approach We Used to Collect and Analyze Data

To answer the six evaluation questions, we obtained documents to provide evidence of service policies and program management activities and conducted structured interviews to ensure that information was consistently obtained from the program management offices. Our data sources are discussed briefly below and more fully in chapters 2 and 3. Table 1.2 gives an outline of the primary data sources by evaluation question.

Table 1.2: The Primary Data Sources for Our Evaluation Questions

Evaluation question	Publications, Office of the Secretary of Defense, and service headquarters	School	Program management office	Lab	Contractor
1. How does DOD define technical risk?	X				
2. What guidance does DOD provide for assessing technical risk?	X	X			
3. How have the services implemented Initiative 11?	X				
4. What are the characteristics of current efforts to identify the technical risks of new systems?			X	X	X
5. How are efforts to identify technical risk implemented?			X	X	X
6. What information on technical risk is available to decisionmakers in the review process?			X		

For question 1, on DOD's definition of risk, we gathered publications that define technical risk, including regulations and other documents specifically about risk assessment for DOD and the three services.

For question 2, on DOD guidance, to gain background information on the approaches to technical risk assessment available within DOD, we used documents and interviews at the Office of the Secretary of Defense and the Defense Systems Management College, the Army Logistics Management Center, the Naval Postgraduate School, and the Air Force Institute of Technology.

For question 3, on Initiative 11, our primary sources were documents (regulations, memoranda, and policy statements that represented official responses to Initiative 11) and interviews with staff in the Office of the Secretary of Defense and with individuals at the headquarters of the three services who were involved in decisions relevant to the initiative.

For questions 4, 5, and 6, on risk effort characteristics, implementation, and information for decisionmakers, the primary data source was an in-depth census of our universe of programs. We gathered documents and interview information from program management offices on the risk-identification efforts performed for major systems under development in the Army, Navy, and Air Force. (We also conducted exploratory interviews with individuals in DOD and at the headquarters of each service.)

Documentation included risk assessments performed for the weapon systems and documents available for the DSARC review. Among the documents required by the DSARC were system concept papers, decision coordinating papers, integrated program summaries, test and evaluation master plans, acquisition strategies, and briefing materials prepared for the DSARC and the services. At each program office, we interviewed the program manager and deputy, contract officer, chief engineer, and others, if any, involved in performing risk assessment efforts. We also interviewed staff at service laboratories and contractors if they performed assessments for the program management office, but we did not seek information from these sources unless the program management informed us of their outside contribution.

For help in answering the last three evaluation questions, we also developed structured interviews when data collection across multiple sites was required. We used separate data collection instruments for the program offices, schools, laboratories, and contractors. We developed a primary interview for program managers, deputy program managers, chief engineers, and other program staff and an additional set of questions, which we used in conjunction with the main interview, for persons who actually conducted risk-identification efforts. We used separate interview forms for contract officers and for program offices in the Army that employed the total risk assessing cost estimate approach. Forms were pretested at 6 program offices during the planning phase of this study. Further information on the data collection instruments is available from GAO's Program Evaluation and Methodology Division.

We selected qualitative data analysis, including a tabulation of variables drawn largely from our interviews in the program management offices, as the approach best suited to the information we gathered. We also analyzed the documents we collected in order to describe the technical risk information they contained.

For a few weapon systems, the program management offices performed two or more risk efforts. For these, an effort was considered primary if it was the one most frequently mentioned by respondents or was the one that had been most recently conducted or met more technical risk assessment criteria than other efforts (see chapter 3). Appendix I mentions a variety of technical risk evaluations that we did not include in our analyses. (Our review was conducted in accordance with generally accepted auditing standards.)

Our Study's Strengths and Limitations

Given its purpose and design, our study has strengths and limitations that should be recognized. One limitation is that the study's accuracy and completeness of data depend largely on the respondents. Whenever possible, information from one respondent was confirmed, and inconsistencies resolved, by checking with other respondents, including former members of the program management staff, and by referring to official program documents. In some instances, however, the structure of the program office or the nature of the risk effort made it impossible to obtain further information; thus, for a few questions in the report, some data are missing.

A second limitation derives from the parameters set by our evaluation questions. The purpose of this study was to discriminate risk efforts on the basis of clear differences in their design and implementation. Our purpose was not to determine whether the efforts were actually used in program decisionmaking or to compare the effectiveness of efforts that do and do not meet various assessment criteria. Accordingly, we did not attempt to link efforts to outcomes such as restructuring programs or reducing cost growth.

A third limitation also derives from our purpose. We examined only the process of addressing technical risk in weapon systems development. We made no attempt to estimate actual risk or the accuracy of statements about risk for the systems. No judgments were made about which systems have high risks or about whether risks should be an impediment to approving the continuance of systems.

The study has noteworthy strengths as well. First, our interviews were with respondents who have a comprehensive range of interests and experiences relevant to this topic, including program managers, milestone reviewers in command offices and in the Office of the Secretary of Defense, and staff members in program offices, laboratories, and contractors. We also interviewed representatives of DOD schools offering courses on risk. In combination, our interviews included respondents who plan, perform, interpret, and review risk efforts and respondents who provide relevant training.

Second, with the exceptions already noted, we covered all major acquisitions now in development. Since these receive DOD's closest scrutiny, we expected risk efforts for these systems to be among DOD's most careful attempts to identify and plan for technical problems.

Third, working from published sources on risk assessment and program management (listed in appendix II), we developed generic criteria for gauging the quality of risk efforts. To our knowledge, no other set of criteria like these exists. While our set is not necessarily definitive, it does offer a meaningful way to discriminate risk efforts and a basis for further refining the criteria.

Finally, this report provides new and important information. Previous studies have not systematically described the characteristics of DOD's risk efforts or the information these efforts provide to decisionmakers. (See, for example, Army Department, 1973, and Williams and Abeyta, 1983.[1]) Ours does, providing a basis for evaluating possible revisions in relevant DOD policies and practices and for planning studies of the effects of risk assessment on program costs and schedules. Appendix III contains comments DOD made on a draft of this report and our response to the comments.

---

[1] Full bibliographical data are given in appendix II.

BLANK PAGE

Chapter 2

DOD's Policies for Technical Risk Assessment

In this chapter, we answer the first three evaluation questions:

1. How does DOD define technical risk?

2. What guidance does DOD provide for assessing technical risk?

3. How have the services implemented Initiative 11?

Current DOD policies call for the acknowledgment and discussion of a system's technical risks throughout the acquisition cycle. Responsibility for assembling and providing technical risk information is placed on the program management office. As a result, reviewers of the system may have the advantage of obtaining information from the persons who are the most experienced with it. One disadvantage is that the program staff may not provide an objective or independent look at the system, although the reviewers need complete and comprehensive technical risk information to make their own evaluations.

The first document required for approving the acquisition of a weapon system, "Justification for Major System New Start," must discuss the maturity of the system's technology with "particular emphasis on remaining areas of risk." Later, at each milestone, decisions made at higher command levels must take technical risk into consideration. This is to be documented as follows.

1. At milestone I, a system concept paper must identify key areas of technical risk, which are to be reduced through research and development, the reduction to be validated through testing and evaluation before milestone II.

2. For milestones II and III, a decision coordinating paper must contain a discussion of the continuing technical risks of the system. For milestone II, this paper must also discuss test and evaluation results and show that all significant risk areas have been resolved and that the technology requires only engineering (not experimental) efforts.

3. For each milestone review, a test and evaluation master plan must describe critical issues to be addressed by testing, including issues arising from technical risk.

4. If all or part of the system's technology has not been demonstrated, then for each milestone review, an integrated program summary must

identify the technical risks and activities that have been planned for reducing them.

5. For each milestone review, a paper called "acquisition strategy" must summarize the technical risks and the plans to reduce or eliminate them.

Further evidence of DOD's concern with technical risk appears in testimony before the Congress. In hearings before the House Budget Committee on February 23, 1983, the undersecretary of Defense for research and engineering stated that DOD was "making realistic assessments of technical and schedule risks and limiting technological advancements to be incorporated in our systems" (U.S. Congress, 1983b, p. 508). On February 27, 1984, in hearings before the House Armed Services Committee, the undersecretary stated that following Initiative 11, "significant progress" had been made toward reducing cost growth stemming from technical risk, citing an effort that "quantifies the cost required to overcome development risk and program the RDT&E [research, development, test, and evaluation] funds needed" (U.S. Congress, 1984, p. 70).

Finally, as we discussed in chapter 1, Initiative 11 called upon the services to improve their technical risk assessments and to budget for technical risk. As a result, analysts inside and outside DOD have developed or identified approaches for assessing technical risk.

How Does DOD Define Technical Risk?

There appears to be no standard definition of technical risk in DOD's documents and regulations or those of the services. In some instances, the term "risk" is used to refer to program risk in general. In other instances, the term refers to one or another component of program risk, such as cost growth, schedule delays, and performance problems. Risk assessment approaches often break program risk into these components. Some approaches deal exclusively with one component; others incorporate more than one within the same model. While each of these risk components is critical to program success and requires explicit attention, they are not independent. As we discussed in chapter 1, technical problems are apparently a major factor in the cost overruns in weapon systems acquisition. Therefore, technical risk is related to cost risk and, in the same way, to schedule risk.

The Defense Systems Management College defines risk as "the probability and consequence of not achieving some defined program goal—such as cost, schedule or technical performance" (Defense Systems, 1983, p. 3). This definition suggests that ratings of technical risk should take into account both the likelihood and the consequences of problems. Accordingly, a problem considered very unlikely might be rated "high-risk" because if it were to occur, its consequences for program cost or schedule would be severe. Combining probability with consequences in a single rating obscures the nature and level of risk from technical problems. In any case, this definition is not binding or even actively promulgated within DOD.

DOD's regulations on milestone documents do not provide a definition of technical or program risk, nor does DOD's directive for managing risk in the transition from development to production (discussed in the next section below). The only service regulation we found with a definition of program risk is Air Force Regulation 70-15. It governs source selection policy and procedures and defines high, moderate, and low risk, slightly paraphrased as follows:

1. High risk is likely to cause significant, serious disruption in schedule, increase in cost, or degradation in performance, even with special attention from the contractor and close government monitoring.

2. Moderate risk can cause some disruption in schedule, increase in cost, or degradation in performance, but special attention from the contractor and close government monitoring can probably overcome the difficulties.

3. Low risk has little potential for causing disruption in schedule, increase in cost, or degradation in performance; normal effort from the contractor and normal government monitoring can probably overcome the difficulties.

Like the definition of risk given by the Defense Systems Management College, the Air Force definitions of risk levels combine the likelihood that a problem will occur with the seriousness of its consequences. Moreover, the Air Force definitions do not require ratings of technical risk distinct from ratings of cost and schedule risks; they combine these components into an overall rating of program risk.

Air Force Regulation 70-15 also requires contractors to identify risks in their proposals. The regulation suggests that the program management office should give the source selection evaluation board that receives the proposals an independent assessment of the risks in advance. However, it does not specify how to assess the risks. The Army and Navy have no corresponding regulations defining risk.

Has Initiative 11 imposed upon DOD a standard definition of risk? Since "technological risk" appears in its title, "Incorporate the Use of Budgeted Funds for Technological Risk," Initiative 11 clearly refers to technical risk, not schedule or cost risk. Two years after Initiative 11 was issued, the deputy secretary of Defense reiterated this point, saying that the services had implemented procedures to budget for "technological risk" (U.S. Congress, 1983a, pp. 252, 270, and 284). Yet TRACE, the total risk assessing cost estimate method recommended by the deputy secretary for this purpose, may focus on cost or schedule risk. It does not require an explicit focus on technical risk or provide a definition of technical risk. (TRACE is discussed in detail later in this chapter.)

In summary, we found no standard definition of technical risk within DOD. The only definitions that do exist are for program risk as a whole, specifying cost, schedule, and performance as three components of risk. Even these definitions are not standard, however, and no regulation sets them for the whole department. (We describe the program offices' various working definitions of technical risk in chapter 4.)

What Guidance Does DOD Provide for Assessing Technical Risk?

Approaches for assessing technical risk can be either quantitative or qualitative, depending on whether statistical probabilities are assigned to a risk element. But all risk assessment entails some subjectivity. In virtually all approaches, experts are asked for subjective judgments of what the risk elements are as well as the likelihood of their occurrence. What distinguishes one approach from another is the information that goes into the subjective judgments (such as test results or professional expertise) and the ways in which the information is obtained, as well as the kind of information requested (for example, a judgment of high, medium, or low risk or a judgment about statistical probabilities).

Quantitative Approaches

Specifically in response to Initiative 11, the Defense Systems Management College published Risk Assessment Techniques: A Handbook for Program Management Personnel (Defense Systems, 1983). The handbook guides program management offices in conducting formal, quantitative risk assessments with various probabilistic approaches. It describes tools and techniques intended for deriving budget figures for risk that can be used more specifically to quantify technical risks as well. Two of the most frequently used quantitative approaches for technical risk assessment, both covered in the handbook, are the "network" and "risk factor" approaches.

The network approach involves modeling the acquisition process for a system as a network, in which the nodes or end points represent milestones in the program and the links between the nodes represent activities that must be carried out in order to reach each end point. The probability of successfully carrying out an activity is usually added to the model. Numerous computer simulations are then performed to evaluate the probability of achieving the goal represented by the network as a whole. Examples of network models are the "venture evaluation and review technique" and "risk information system and network evaluation technique," both of which may also be used to address schedule risk and cost risk.

The risk factor approach was developed to support budgeting for technical risk. In this approach, all elements of a system and their associated costs are identified in a baseline cost estimate. A "risk factor" is then determined for each element associated with risk in the weapon system. This factor is a number by which the estimate should be increased to account for a technical problem if it were to arise. The estimate and risk factors are determined by individuals with expertise in the technology required for the weapon system.

Another quantitative approach is decision analysis. Also covered in Risk Assessment Techniques, it requires the development of a decision "tree" (a kind of flow diagram) in which sequences of supporting decision steps are laid out in branches. This aids in identifying uncertain occurrences in the chain of decisions. Probabilistic performance simulation, an approach not covered in the handbook, is the application of a computer simulation to equations representing factors that can contribute to technical risk. These factors may be specified by government requirements or derived from specific system performance goals.

Such risk assessment approaches as these can be used in different aspects of the acquisition process. The program management offices can use them for budgeting, as in the use of TRACE to budget for risk, and for day-to-day program management, as when decisions about program alternatives must be made. The assessments can also be used in decisions made at levels above the program office, for both budgeting and making realistic decisions about the technology of the weapon system.

Assessments of risk can also help determine if program milestones have been scheduled appropriately.

Qualitative Approaches

The Defense Systems Management College handbook focuses on quantitative approaches, but qualitative techniques are perhaps more widely used and are generally simpler to apply. Some qualitative approaches provide only a single risk rating for a system as a whole, but a generic approach recommended by LTV Aerospace and Defense Company requires a comprehensive examination of program technical risk areas. It involves the following steps. (1) Develop a decision tree to display the hierarchy of critical system requirements. (2) Specify the parameters for tracking technical performance during the program. (3) Review the system design and system requirements, preferably by breaking the work down into its essential structure, to ensure that all elements are examined. (4) Establish written criteria to define levels of risk. (5) Ensure that program managers are aware of and understand the approach, status, and results of the assessment. (6) Document the risk assessment approach and results.

Rather than using the probabilities that are estimated for quantitative ratings, qualitative approaches assess risk either through descriptive information (identifying the nature and components of risk) or through an ordinal scale (high, medium, and low, for example, or red, yellow, and green). However, qualitative ratings are like quantitative ratings in that they are usually based on the judgment of experts.

Other DOD Efforts to Address Risk

Another approach to risk, known as risk management, does not assess risk. Risk management, because it identifies and reacts to problems as they arise, is not prospective in the way risk assessment is. Risk management is the implementation of strategies to control or monitor program risks, and it may follow a technical risk assessment and focus on risks the assessment identified. Moreover, risk management does not necessarily provide explicit coverage of technical risk; it may center on schedule or cost considerations.

In a recent effort toward risk management in a particular phase of the acquisition process, DOD explicitly recognized the distinction between risk management and risk assessment. DOD's January 19, 1984, directive 4245.7, entitled "Transition from Development to Production," requires that all systems in development and production are to implement a formal program of risk evaluation and reduction. It calls for the assessment of program risk throughout the acquisition cycle and charges program management with the execution, and the DSARC with the enforcement, of the provisions.

The resource document for implementing the directive is called "Solving the Risk Equation in Transitioning from Development to Production" (DOD manual 4245.7-M) and was developed by a Defense Science Board task force under the leadership of the deputy chief of naval material for reliability, maintainability, and quality assurance. The document includes a series of templates, geared to the most critical events in the design, test, and production elements of the industrial process, but it is aimed at risk management and does not provide a technical risk assessment approach for program management offices.

To complement "Solving the Risk Equation," the task force developed "Best Practices for Transitioning from Development to Production," another manual in which technical risk assessment is recognized as a separate function essential to the successful development of a weapon system. The manual suggests ways to avoid pitfalls in risk management but does not describe or recommend approaches for risk assessment.

In addition to looking for specific approaches, we looked for more generic definitions of and criteria for technical risk assessment. We found that DOD has not established a generic definition or generic criteria. After reviewing research in organizational management as well as risk assessments by DOD and private industry and after consulting with a number of experts in technical risk assessment, we developed five criteria for defining it: prospective assessment, planned procedures, explicit attention to technical risk, documentation, and reassessment in each acquisition phase.

If an assessment is to be called "technical risk" assessment, all five of these criteria must be present. For instance, the qualitative and quantitative approaches we described can all be used to perform technical risk assessments, but using them does not guarantee that an assessment meets the five criteria. A very sophisticated analysis that had not been documented, for example, would not be a technical risk assessment under our definition. This is because an undocumented analysis is not very useful for decisionmaking. (Each of these criteria is discussed in detail in chapter 3.)

In summary, many technical risk assessment approaches, quantitative and qualitative, are available within DOD. But there is no official policy to guide program managers and analysts in the selection of suitable approaches, and there are no generic criteria defining an adequate technical risk assessment, independent of each individual approach.

How Have the Services Implemented Initiative 11?

In 1981, the deputy secretary of Defense conducted a systematic review of DOD's acquisition process, with the objectives of reducing costs, making the process more efficient, increasing program stability, and reducing the time required for system development. From this review evolved 32 initiatives, including, for example, the use of more economical production rates and earlier testing of systems. Initiative 11 required the services to increase their efforts to quantify technical risk. In particular, the initiative required the services to adopt the Army's total risk assessing cost estimate (TRACE) method or propose an alternative. Reporting on the status of the initiative in a June 8, 1983, memorandum, the deputy secretary of Defense stated that procedures to budget for risk had been implemented by the services. "This initiative is now considered completed," he said. After a short description of TRACE, what each service actually did, as the services reported it, is discussed below.

The Army developed the total risk assessing cost estimate method in 1974 in order to be able to add an incremental dollar figure to the baseline cost estimate of a program that would account for uncertain events and to be able to base a justification of this figure on sound estimation and analysis. The dollar figure is calculated by identifying uncertain events for the various subsystems or components in a program and estimating the amount of money that would be required to cover additional costs associated with each potential problem. Once these costs have been calculated (by means of various techniques including some described above), TRACE provides an estimate that represents the tradeoff between funding only for costs of the program that can be identified with certainty and funding for all possible risks.

According to TRACE guidelines, the risks that may be included in TRACE calculations are design changes to resolve technical problems, rescheduling to resolve technical and budgetary problems or the late delivery of components or materials, additional testing of design corrections and hardware to support them, nonnegligent human error, and program termination.[1] Many of these risks, of course, are not necessarily technical in origin. Thus, to fulfill Initiative 11, analysts using the TRACE procedure (or any alternative) must distinguish technical risks from other risks and then quantify the technical risks. One way to do so is to estimate numerical probabilities for the occurrence of various technical problems. In network analysis, the probabilities are used as input for calculations of overall technical risk. They can also serve as a basis for projecting the cost implications of each problem. A second and more direct way to quantify technical risks is simply to estimate the amount needed to cover each possible problem and use this amount as a quantitative indicator of risk.

Army

Originally, TRACE funds were calculated for the preproduction phases of system acquisition—research, development, testing, and evaluation—because much of the risk associated with weapon system development arises in the early stages. In its internal budgeting, the Army now applies TRACE to the production phase for some systems as well. The Army's response to Initiative 11 was to continue the previously instituted TRACE program. Program offices were not directed to distinguish technical risk in their TRACE analyses or to quantify the costs associated specifically with technical problems.

Navy

Responding to Initiative 11, the Navy established a pilot program to evaluate the use of TRACE with six systems. The opinion of the coordinator within the Naval Air Systems Command, where the pilot program was set up, is that the methods for calculating risk funds are so complicated and require so much time that, when they are affordable, they must be done by outside experts. Consequently, he stated, the outsiders become the risk experts, and program managers gain little knowledge. The Navy has confined TRACE to preproduction phases and has never moved beyond the pilot effort. Some of the systems in the pilot program have dropped the use of TRACE and others are no longer eligible, having moved into production. The pilot effort did not require that TRACE analyses pay explicit attention to technical risk.

---

[1] Costs for modifications that result from changes in the statement of technical requirements, the effects of inflation, and additional costs stemming from pay increases are not considered in TRACE calculations.

Air Force

The Air Force chose not to adopt TRACE for dealing with risks, and therefore none of its programs has TRACE funding. The response of the Air Force to Initiative 11 was to state its satisfaction with the cost estimation procedures already in use for quantifying risks, saying that it saw no advantage to the TRACE approach. The Air Force issued no requirement for explicit attention to technical risk in those procedures. Initiative 11 thus changed no Air Force policies.

Initiative 11 and the Defense Systems Acquisition Review Council

According to the director of major systems acquisition in the office of the undersecretary of Defense for research and engineering, Initiative 11 led to no changes in procedures or documentation that the DSARC uses to evaluate the development of systems.

Summary of Initiative 11

Initiative 11 was intended to promote the quantification of, and budgeting for, technical risks. In response to Initiative 11, one Navy command (the Naval Air Systems Command) tried a small TRACE pilot program. The Air Force made no changes from the outset, and the Army has maintained the TRACE program at its earlier status. Yet, as we noted earlier, to fulfill Initiative 11, the services would need to conduct analyses that distinguish technical risks from other risks and quantify the technical risks by means of probability or cost estimates. TRACE does not necessarily do so, and none of the services has instructed its program offices to use TRACE, or any alternative, in ways that would deal specifically with technical risks. Nor has the DSARC adopted any procedure or requirement that would entail distinguishing and quantifying these risks. The net effect of Initiative 11 on technical risk assessment procedures has thus been negligible.

Summary

We found that the Department of Defense has general policies calling for technical risk assessment, but the policies do not provide any standard DOD definition of program risk or technical risk, and they offer no guidance for designing or selecting suitable assessment approaches. Regulations governing system documentation require that technical risk be addressed but do not define technical or program risk.

Neither the DSARC nor the services have responded to Initiative 11 by requiring assessments that distinguish technical risks from other program risks or quantify the technical risks.

Chapter 3

Differences in How the Program Offices Address Technical Risk

In this chapter, we describe how the 25 program management offices we examined attempted to identify the technical risks of the 25 systems. Because of Initiative 11 and the Defense Systems Management College handbook on risk assessment, we expected to find the offices assessing technical risk in quantitative (or probabilistic) terms and earmarking funds to cover that risk. Because of DOD requirements for milestone reviews, we also expected to find documents explaining how risk is assessed and how the amount of funds needed to cover risk is calculated. We believed that some offices might identify risks in other ways as well, perhaps using qualitative approaches like those described in chapter 2 or setting up a risk management system to pinpoint technical problems as they arise.

In short, we expected considerable variability in approaches to technical risk and wanted to be sure that our data collection did not miss this variability. Hence, in our interviews and document reviews, we investigated every effort of the program offices to identify technical risks. We have used the expression "risk effort" to refer to whatever approach we found in the 25 offices, reserving the term "technical risk assessment" for efforts that met the particular criteria described below.

In this chapter, we cover evaluation questions 4-6:

4. What are the characteristics of current efforts to identify the technical risks of new systems?

5. How are efforts to identify technical risks implemented?

6. What information on technical risk is available to decisionmakers in the review process?

To answer question 4, we first discuss the number of program offices that used quantitative efforts to budget for risk. Then, to provide a basis for describing efforts in all 25 program offices, we establish five criteria that are essential in technical risk assessment and discuss the number of program offices meeting these criteria. To answer questions 5 and 6, we consider all efforts we found, whether or not they met all five criteria.

Answers to a few study questions from respondents inside an office were inconsistent in ways we could not resolve by referring to the majority answer or program documents. Other information we needed was simply not available, and where this is relevant, we note it. For most of our questions, though, an overall response could be coded for all or almost all the offices.

What Are the Characteristics of Current Efforts to Identify the Technical Risks of New Systems?

To answer this evaluation question, we first describe quantitative efforts to budget for risk and then describe the efforts we found in all 25 offices.

Quantifying and Budgeting for Technical Risk

Despite the availability of the Defense Systems Management College risk assessment handbook, and despite the deputy secretary's assertion that Initiative 11 has been implemented, none of the offices we examined had performed a quantitative effort and used it for the purpose specified in Initiative 11—to calculate the funding necessary to cover technical risk. One office, responsible for the Army's Short-Range Air Defense Command and Control system (SHORAD C2), did perform a quantitative assessment of technical risk but then supported its application for risk funds with an entirely different assessment. The latter assessment used TRACE to calculate cost risk from potential schedule slippages, in which technical risks were not quantified or even explicitly considered.

Assessment Criteria and Risk Efforts

Although we found that no quantitative efforts had been used for risk budgeting, we found other efforts in all 25 program offices and collected descriptive information on them. We imposed no definition of "risk effort" but simply asked respondents to describe relevant activities, however they defined this expression. If any part of their effort had been handled by sources outside the office—for example, service laboratory staff or contractors—we interviewed these sources as well.

As we reported in chapter 2, DOD has no policy calling for a particular assessment approach or specifying, in general terms, what sorts of assessment are acceptable. Since we could not compare the efforts we found to any official DOD standard, we reviewed the research on organizational management as well as risk assessments conducted in DOD and the defense industry (given in the bibliography) and consulted methodologists familiar with the area. From this review, we developed five criteria that can be considered essential in the assessment of technical risk:

1. prospective assessment: Possible future technical problems are considered, not just current problems.

2. planned procedures: Assessment is planned and systematic, not incidental.

3. attention to technical risk: There is explicit attention to technical risk, not just to schedule or cost risk with consideration of technical risk left implicit.

4. documentation: At a minimum, technical risk assessment procedures and results are written down in some form.

5. reassessment in each acquisition phase: New or updated assessments are made in order to detect changes in risk during a system's development.

These criteria are not necessarily definitive, but they do reflect relevant, attainable characteristics and thus provide a reasonable basis for appraising the quality of risk efforts. Moreover, since we did not attempt to gauge the accuracy of risk ratings or the suitability of particular assessment approaches, these five criteria represent a minimum standard of quality. As we noted earlier, we reserve the term "technical risk assessment" for efforts meeting all five criteria.

Below, we briefly discuss each of the five criteria and then cite the number of program offices with risk efforts that met each one. Then we discuss efforts meeting all five. Table 3.1 shows the criteria that were met for the 25 systems in table 1.1.

Table 3.1: DOD Risk Efforts Rated on the Technical Risk Assessment Criteria

Service and system	Prospective	Documented	Planned	Explicit	Reassessed in each phase
Army					
AHIP	X	X	X	X	
M1A1	X		X		X
MLRS/TGW	X		X	X	
RPV	X	X	X	X	X
SHORAD C2	X	X	X	X	X
Navy					
ALWT		X	X	X	
ASPJ			X	X	X
ASW SOW	X	X	X	X	X
ATRS				X	X
CV-HELO			X	X	X
HFAJ	X				X
JTIDS	X				
SUBACS	X	X	X		
T45TS		X	X	X	X
Trident II (D5)			X	X	X
V-22 Osprey				X	X
Air Force					
AMRAAM	X				
ASAT	X	X	X	X	
C-17A			X	X	X
I-S/A AMPE	X				X
JTIDS	X				X
JSTARS	X		X	X	
Mark XV IFF	X	X	X	X	
NAVSTAR User Equipment			X	X	X
SRAM II	X		X	X	
Total	**16**	**9**	**18**	**18**	**15**

Prospective Assessment

To be useful predictively, technical risk assessment must identify risks well before they become actual problems. An assessment early in the development process—listing risk areas and perhaps estimating degrees of risk as well—can provide a systematic foundation for further analysis and revision as a system moves through acquisition. But an assessment based, for example, on tests conducted just prior to the production decision (milestone III) does not assess the risk that the problems will occur. It uncovers the fact that problems have already occurred.

Prospective risk efforts were conducted for 16 (or 64 percent) of the systems. For the 9 others (or 36 percent), technical problems were identified as they arose, often through risk management systems, but risks were not identified in advance.

Planned Procedures

Technical risk assessments must be carefully planned—that is, risks must be identified by deliberate, systematic procedures. Without planning, technical staff members may overlook potential risks, or some may believe a system's components to be high in risk while others believe the same components to be moderate or low in risk. Such discrepancies could easily go unrecognized until a risk turned into a major problem. Technical risk assessment cannot consist of only unplanned, occasional discussions of risk in staff meetings or other ad hoc procedures.

We found 18 systems (72 percent) with planned efforts. Ad hoc efforts were made for 7 (28 percent); risk was considered when staff members or outside entities brought it up, but risk efforts were not a planned activity.

Explicit Attention to Technical Risk

Some assessments combine the technical, cost, and schedule components of overall program risk. For example, the Army's TRACE procedure uses "high," "low," and "most likely" cost estimates for each subsystem, producing an overall estimate of cost risk for the system as a whole. The sources of subsystem cost risk, including possible technical problems, may not be identified explicitly; if not, the assessment will not be useful as an indicator of the system's technical risk.

In our study, risk efforts for 18 systems (72 percent) identified technical risks explicitly. Efforts for the 7 others (28 percent) considered technical risks only implicitly, in cost risk or schedule risk assessments, or measured overall program risk without isolating its component of technical risk.

Documentation

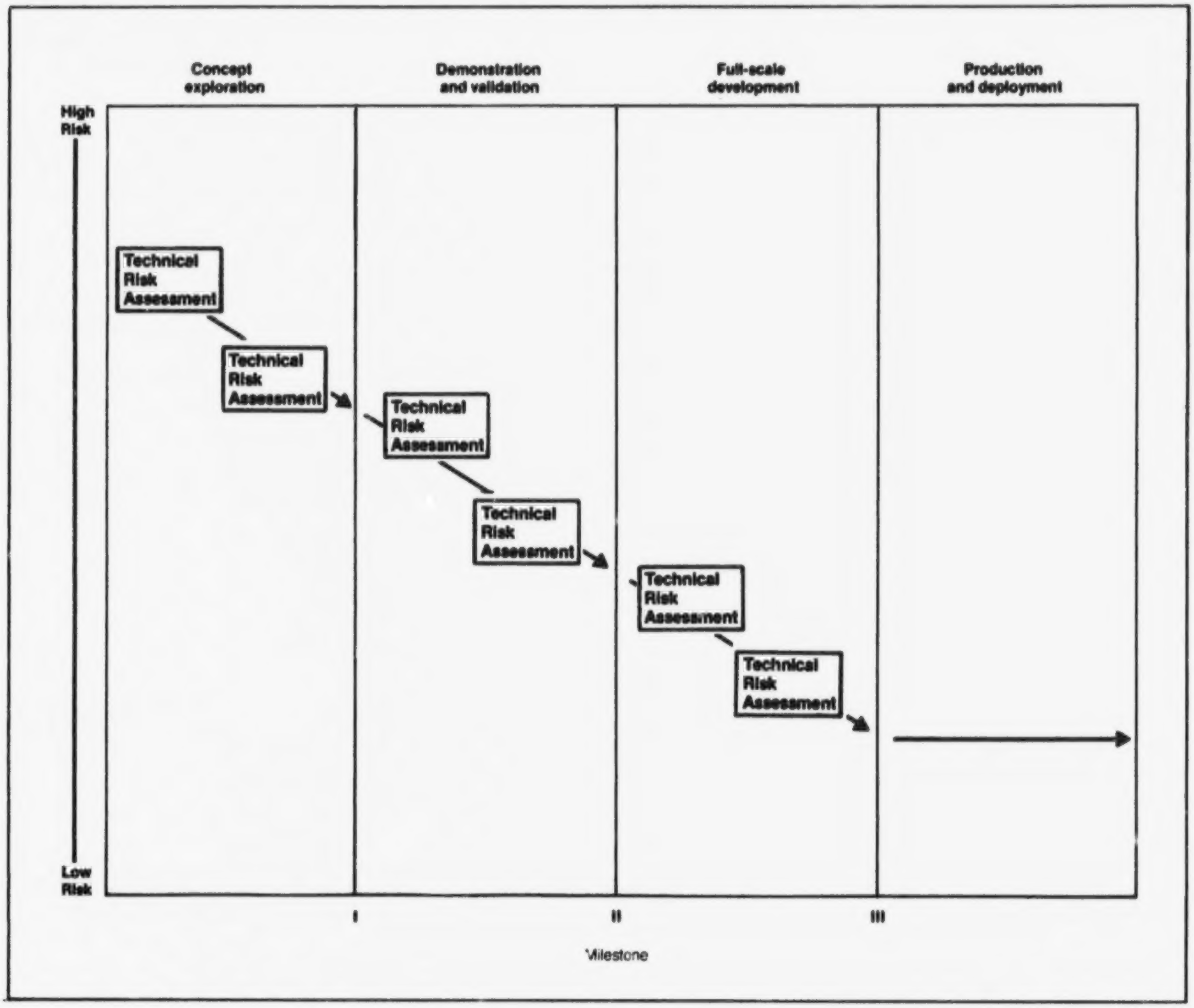
Technical risk assessments must be documented, so that program managers, technical staff, and reviewers can monitor the procedures followed to identify risks and can verify the results. This capability is especially important for program managers and staff newly assigned to an ongoing development effort and for milestone reviewers who might need to know specific details.

For only 9 of the systems (36 percent) in our study were the risk efforts documented. For the majority (64 percent) technical risk was addressed in staff meetings and program planning without recording the process or results. (In these cases, our data on risk efforts were obtained from interviews, as we noted in chapter 1, with program office staff.) All the program offices provided some risk information in the milestone review documents, but it was insufficient (for reasons we delineate in the section below on technical risk information available to decisionmakers).

Reassessment in Each Acquisition Phase

Movement from one phase to the next is based on the status of a system's technical problems. Thus, program management staff and reviewers must be able to track the identification of risks during a system's development and gauge, from data such as test results or expert judgment, how much progress has been made. Risks must first be assessed early in concept exploration and then be reassessed later in the same phase, so that decisionmakers at milestone I can know what risks have been identified and how much progress has been made toward their resolution. Since system development is ongoing and milestone reviews may lead to design changes, another assessment would be due early in the next phase. The same logic supports further reassessment, leading ultimately to the milestone III decision for production and deployment of an operational system. In short, technical risk assessments should be conducted at least twice in each acquisition phase, one early and another late, to support staff and review decisions regarding whether and how to proceed to the next phase. Each reassessment may be an entirely new effort or update the previous one. Figure 3.1 depicts this criterion.

Figure 3.1: The Criterion of Reassessment in Each Acquisition Phase


Concept exploration
Demonstration and validation
Full-scale development
Production and deployment
High Risk
Low Risk
Technical Risk Assessment
Technical Risk Assessment
Technical Risk Assessment
Technical Risk Assessment
Technical Risk Assessment
Technical Risk Assessment
I
II
III
Milestone

We were unable to define a time for early and late assessment in each acquisition phase for each system. Program management offices skipped at least one milestone for many systems. For others, because development had begun several years ago or milestone review dates had slipped, we could not establish early or late times with precision. An alternative approach was simply to ask whether risks were assessed at least twice in each phase by means of annual updates or the like. We could not be sure that there had been one early and one late risk effort in each phase, but we could determine that one occurred later than another and that the program management staff therefore had had an opportunity to detect any changes in risk.

Since many of the programs in our study skipped one or two early phases or had not yet reached full-scale development, we determined whether a program management office had assessed risk at least twice in each phase a system had reached and not skipped. Of our 25 offices, 15 (60 percent) had done so. Most of these offices (12 of the 15) performed risk efforts as an ongoing part of program management.

Risk Efforts Meeting All Five Criteria

Only 3 (12 percent) of the risk efforts performed for these systems fulfilled all five criteria (as we showed in table 3.1): the Army's Remotely Piloted Vehicle (RPV) and Short-Range Air Defense Command and Control System (SHORAD C2), and the Navy's Antisubmarine Warfare Standoff Weapon (ASW SOW). The prospective decision risk analysis for the RPV was conducted according to a planned schedule, first in 1981 and subsequently in three annual updates. The 1981 and 1982 analyses focused explicitly on technical risk. For the 1982 analysis, staff members were asked to rate each of the RPV's subsystems (target location, air-vehicle endurance, and so on) on a six-point scale of technical risk, ranging from "none or very low" to "unacceptably high." The ratings were anchored to quantitative estimates of failure and verbal descriptions of risk. Systems analysts, assigned to the program management office according to a matrix organization, aggregated ratings from individual staff members to arrive at overall qualitative ratings. Documentation described the process and results in detail. (See table 3.2).

Table 3.2: Technical Risk Rating Scale for Remotely Piloted Vehicle

Qualitative label	Probability of failure	Description
None or very low	0– 4%	Fully developed and in production; meets military specifications
Low	5–15	Fully developed and producible but not yet in production; meets military specifications
Moderate	16–30	Needs little further development; has not met military specifications
High	31–40	Needs further development and debugging
Very high	41–50	Has been designed but needs extensive development
Unacceptably high	51 +	Is theoretical and may exceed the state of the art

Source: W. Bodden et al., Decision Risk Analysis: Remotely Piloted Vehicle (St. Louis: Army Aviation Research and Development Command, 1982), p. B-2.

The prime contractor for the ASW SOW provided prospective risk assessments, focusing explicitly on technical risk. Judgments of the likelihood of the system's meeting performance requirements were collected from prime contractor and subcontractor staff and then documented in the form of qualitative ratings of risk (high, moderate, and low). Reassessments were conducted regularly and according to plans negotiated with the program office staff.

The SHORAD C2 program office handled its risk assessments in different ways as the system moved through development. For the 1985 reassessment, the program office brought in a support contractor to collect prospective risk data from program engineers and other specialists. The data focused explicitly on technical risk and were expressed as quantitative ratings of the probability of technical failure for each subsystem. Ratings were aggregated to produce a qualitative estimate of program risk for the system as a whole. As planned, the support contractor fully documented the process and results for the use of the program office.

Risk efforts for 15 other systems met three or four of our five criteria, and efforts for all systems met at least one. Since a technical risk assessment, as defined here, must fulfill all five criteria, we have not provided a detailed description of efforts that did not fulfill one or another individual criterion. But two examples will illustrate what we typically found. For the Air Force Inter-Service/Agency Automated Message Processing Exchange (I-S/A AMPE)—a highly sophisticated system for command, control, communication, and intelligence—program management staff gathered information on technical risk through various ad hoc methods, such as vendor conferences and surveys (to evaluate design alternatives) and reviews by cost analysts, users, and laboratory representatives. But this input did not focus explicitly on technical risk, nor was it documented. For the Army's M1A1 tank, three TRACE analyses were performed. The analyses produced "high," "low," and "most likely" cost estimates for each of the M1A1's subsystems, but no explanation of technical risk was provided for any one subsystem. Staff members reportedly considered technical risk when providing TRACE input, but this also was not documented.

Differences Between the Services

For three of the five criteria, we found differences between the services. Most Army and Air Force efforts were prospective, but a majority of those in the Navy were not. Further, the Army usually documented its efforts; the Navy and Air Force usually did not. Finally, the Army and Navy usually repeated their efforts within acquisition phases; the Air Force usually did not.

Despite the higher incidence of Army efforts meeting these three criteria, program management offices of neither the Army nor the two other services, in the majority, met all five criteria.

In summary, program offices for none of the 25 systems performed the sort of risk effort suggested by Initiative 11—a quantitative assessment of technical problems for use in risk budgeting. Using a generic concept based on five essential criteria, we found only 3 program offices performing efforts that met all five criteria. The remaining 22 addressed risk in some way but did not fulfill at least one of the criteria.

We reiterate that in our study we did not evaluate the effect of risk efforts on cost or schedule problems. Hence, we cannot say whether quantitative assessments or risk efforts meeting all five criteria have actually helped reduce cost growth or time delays. But risk efforts in most program offices cannot have served well as technical risk assessments. The lack of documentation—documentation is essential for the needs of decisionmakers—was the most common flaw.

How Are Efforts to Identify Technical Risk Implemented?

In this section, we describe how the program management offices conducted their risk efforts, regardless of whether they met all five criteria for technical risk assessment. From our review of research on organizational management and risk assessment, we concluded that implementing a risk effort entails at least three decisions. For each decision, the persons implementing the effort select one of the options shown in table 3.3.

Table 3.3: Decisions and Options in the Implementation of Risk Efforts

Decision	Option
Format for rating risk	Narrative description Qualitative rating Quantitative rating
Scope the ratings will cover	All subsystems Selected subsystems System as a whole
Input collection procedure	Single rater Group discussion Independent raters

There are, of course, implementation decisions other than what format will be used to rate risk, what scope the ratings will cover, and how data on risk will be collected. One is how much staff time will be devoted to an effort. But it is for these three decisions that particular options (specified below) are most likely to produce accurate and useful results.

Various program circumstances can constrain the choice of implementation options. For instance, the decision regarding procedures for collecting data depends partly on the time and staff skills available for this task. Similarly, the decision on rating format depends partly on the complexity and maturity of the system being developed. Accordingly, for each implementation decision, we have indicated the preferable option and report the number of risk efforts for which this option was selected. But we do not suggest that all efforts should be implemented in the same way, and we have not included any implementation option in our criteria for gauging an effort's quality.

Rating Formats

The three options for deciding how to rate the technical risks associated with a system are narrative, qualitative, and quantitative. Narrative information describes potential problems that may preclude reaching performance requirements; sometimes it also indicates the source of each problem and possible solutions to it or design alternatives. An example is the narrative description of risk associated with a component of the Army's Advanced Helicopter Improvement Program:

> "Both [contractor alternatives] have flown a MMS [mast-mounted sight] on their aircraft . . . and have demonstrated ranges and stability compatible with [system] requirements . . . . [But it] may be difficult to optimize stiffness and weight . . . . The

MMS could impart high main rotor blade bending loads. The main rotor blade balancing/tracking could be difficult . . ." (Fox, 1981, p. A-16).

Qualitative estimates for the likelihood of not meeting performance requirements are usually expressed in an ordinal rating—from high to moderate to low—or in a coded ordinal rating—in which, for example, red is equivalent to high, yellow to moderate, and green to low. The Navy's Joint Tactical Information Distribution System, for example, coded easily solved problems green, possible major problems yellow, and any major problems that seemed potential "show stoppers" red.

Quantitative estimates of risk use a fraction expressed as a decimal to represent the probability of meeting or not meeting performance requirements. One instance of this is in the effort for the Air Force Antisatellite Weapon. The program office rated the probability of success for each ASAT subsystem and then aggregated the figures to produce an overall probability of success.

Narrative ratings have the advantage of content; they describe the potential problem, its sources, and its possible solutions. But the narrative alone does not indicate how raters would estimate the level or magnitude of risk. Qualitative and quantitative estimates do indicate levels of risk. Such estimates alone, however, lack the content provided by narrative descriptions. Systems that are well into development or not very complex might not require both a discussion of risk elements and a specification of risk levels. But, in general, the most informative format would combine narrative information with either qualitative or quantitative ratings.

Only narrative ratings were used for 5 systems (20 percent) in our study. Discussions of risk in the Navy's Trident II program office, for instance, focused on the engineering aspects of technical problems but did not ordinarily entail qualitative or quantitative ratings. Fifteen systems (60 percent) were rated for risk in qualitative terms without narrative details. Three systems (12 percent) were given quantitative ratings without narrative support.

A narrative was combined with qualitative or quantitative ratings or both for 4 systems (16 percent). For the Army's AHIP, narratives for subsystem risk, like the narrative quoted above for the mast-mounted sight, were accompanied by ordinal ratings.

The services took different approaches to rating risk. The Navy tended to use qualitative ratings only; the Air Force provided either narrative information or qualitative ratings. The Army usually rated risk in quantitative terms, but it combined quantitative with qualitative terms in one risk effort and with qualitative and narrative information in two efforts. The Army's greater reliance on quantitative ratings is not simply an artifact of the TRACE analyses it used to budget for risk but can be accounted for by efforts other than TRACE. However, the Army's familiarity with TRACE may help explain its more frequent use of quantitative technical risk ratings.

Rating Scope

Efforts to assess risk may focus on a system as a whole or on subsystems such as hardware components or software subroutines. All subsystems may be assessed for risk or only those for which there seems to be some uncertainty regarding performance. Except perhaps for systems that are relatively mature or simple, an effort covering all subsystems is likely to be more useful than one covering only the system as a whole or only some of its subsystems. Attention to the system as a whole may produce an accurate estimate of overall risk but will not by itself identify the more problematic subsystems. Similarly, an effort incorporating only selected subsystems will not produce an estimate of risk overall, and it may not identify the subsystems that were not selected or report the reasons for the selection.

For 2 systems (8 percent) efforts were conducted only for the system as a whole. For 11 (44 percent) risk was apparently rated for selected subsystems; for 10 (40 percent), it was rated for all subsystems.

Differences emerged in scope. The Navy usually covered some but not all subsystems; the Air Force most often covered all. In no case did the Army gear an effort to a system as a whole but instead assessed all and selected subsystems.

Procedures Used to Collect Data on Technical Risk

The procedures that are used to collect data can affect the comprehensiveness and completeness of the input to an assessment as well as the validity of the consequent output. One person may competently identify and rate risks. But if time and resources permit, several raters working as a group, each with particular experience and areas of expertise, are more likely to produce more accurate input, especially if the raters' assumptions are spelled out and technical details as well as possible solutions are provided. Communication among raters can generate new insights, transfer information, and force a reconciliation of divergent views. Input can be collected in a staff discussion of technical issues or in a survey (using interviews or written questionnaires).

In a survey, input is collected from independent raters and then tabulated, and discrepancies are resolved. The advantage of input from several raters working independently over group discussion is that group pressures and time constraints do not prematurely close issues requiring extended attention. Thus, for all but the most mature and least complex systems, input from several independent raters is preferable.

Risk efforts for 3 of our systems (12 percent) relied on one person to handle the effort. Another 17 (68 percent) collected data from two or more raters, and 14 of these held at least one meeting at which technical risk was discussed. Five (20 percent) collected input from independent raters. (Two used both staff discussion and independent raters.)

Program Circumstances and Implementation

For format, scope, and input procedure, we have cited the options most likely to generate useful information on risk. We also found that few of the program management offices selected these options when they implemented their efforts. But, as we noted above, circumstances such as available staff time and a system's complexity can affect implementation decisions. We did not attempt to rate such circumstances, since their measurement would be highly subjective and imprecise. Therefore, we cannot be certain that the implementation decisions of any of the offices were either appropriate or inappropriate.

At the very least, however, a program office should consider its system's complexity and maturity when making these decisions. If implementation options are selected solely in response to staff availability and other constraints not specific to a system itself, one cannot be confident that the results will be the most useful possible in the further development of the system. An office handling a complex new system, for example, should at least consider performing quantitative analyses in which the risks associated with all the subsystems can be precisely aggregated. It might be more appropriate for another office, managing enhancements to an existing system, for example, to require only a brief description or qualitative rating for each enhancement.

In our study, respondents cited a wide range of reasons underlying the implementation of their risk efforts. Among those most frequently cited were staff experience with similar efforts, confidence in the results, and requirements imposed at higher command levels. In only 6 offices (24 percent) did a respondent say that features of the system itself were considered.

Summary of Implementation

Since implementation options depend partly on program circumstances, we have not attempted to specify any essential criteria for implementation. But apparently few offices considered program circumstances when they implemented their risk efforts, and few offices selected the options that are in general most likely to produce accurate and useful results.

What Information on Technical Risk Is Available to Decisionmakers in the Review Process?

To answer the question on the availability of information on technical risk for those who make decisions at the milestone reviews, we reviewed documents and briefing materials (minutes and scripts as well as charts) prepared by program management offices to describe their technical problems and plans. As we noted in chapter 1, the documents required at milestone reviews include the system concept paper, decision coordinating paper, test and evaluation master plan, integrated program summary, and a paper on acquisition strategy. As we discussed in detail in chapter 2, DOD regulations specify that each document must include information on the technical risks posed by a system or the progress of risk reduction.

We requested official copies of these documents by name and briefing materials by milestone. We also requested other technical documents that were available to reviewers, such as mission element need statements, program management directives, and technical advisory panel reports. Some documents were missing from a few offices, especially for systems that had skipped or not yet reached a milestone and that had passed a milestone before the requirement for specific documents had been established. Other documents were available but excluded from the analysis if the relevant milestone date could not be pinpointed or the milestone had been skipped or not yet reached. When we were provided with several versions of one document (for example, an original for milestone I and its later update), we included each version in the analysis. Across all the offices, we examined 29 milestone documents and 17 sets of briefing materials.

Sources and Types of Information

Most milestone documents included information on technical risk: 80 percent at milestone I and 76 percent at milestone II. Although DOD did not meet its requirement for technical risk information in all these documents, for each system at each milestone there was at least one document providing such information. Further analysis indicated, however, that the information on risk was inadequate. In almost all the documents (none of which had quantitative ratings), the information was a narrative or a qualitative rating of risk for the system or subsystems. Few documents specified an effort's scope or analytical approach at either milestone. (See table 3.4.)

Table 3.4: The Sources and Types of Information on Technical Risk at Milestones I and II

Document	Contains technical risk information	Gives technical risk rating	Cites approach	Cites scope
Milestone I				
Test and evaluation master plan	25%	25%	0	0
System concept paper	100	100	0	0
Acquisition strategy paper[a]	100	100	0	20%
All documents	**80%**	**80%**	**0**	**7%**
Milestone II				
Test and evaluation master plan	60%	50%	10%	10%
Decision coordinating paper	80	80	0	0
Integrated program summary	50	50	0	0
Acquisition strategy paper[a]	100	100	0	0
All documents	**76%**	**72%**	**3%**	**3%**

[a] Includes documents entitled "Acquisition Plan."

For example, the test and evaluation master plan is supposed to list critical issues to be resolved by testing—issues arising from operational requirements and from technical risk. When a plan lacks a description of the risk effort or ratings of the risk associated with critical issues, readers may know what issues are considered critical but will not know (or can only infer) the level of technical risk associated with each issue or the quality of the risk effort for that system. For milestone I, 75 percent of the plans lacked explicit risk information of this sort; for milestone II, 40 percent lacked it.

In another analysis, we examined all the documents the offices provided us, including documents not required for milestones and documents for which no milestone date could be pinpointed. The pattern of results for documents overall duplicates the pattern we found for only the milestone documents: among the total of 119 documents, 64 percent provided risk information, usually ratings but rarely a description of scope or approach.

We examined minutes and scripts for briefings in order to determine what sort of technical risk information was provided to reviewers orally. In most cases, this information took the form of charts showing risk ratings for subsystems or a system overall. For a 1984 DSARC review of the Navy T45TS, for instance, briefing charts provided a qualitative risk rating (low to moderate) for the system as a whole. Charts used for a 1984 review of the Air Force Mark XV IFF combat identification system did not contain qualitative risk ratings but did describe sources of technical risk and design approaches for various subsystems. At milestone I, 43 percent of the briefing materials provided technical risk information, which consisted of risk ratings. None cited the scope or approach of an effort. At milestone II, 50 percent cited risk ratings, and only rarely were scope and approach cited.

In summary, DOD regulations require that all milestone documents include information on technical risk or risk reduction. Most of the documents we reviewed for this study included such information, but some did not. More importantly, the risk information that was available in these documents rarely indicated the scope of the effort or the analytical approach—two items critical to a thorough evaluation of the technical risks posed by a system. The briefing materials we examined suggest that risk information was often not provided orally, although it is possible that reviewers raised questions about risk at the briefings. The information generally provided was a rating of technical risk, but as with system documents, briefing materials rarely specified the scope of the rating and the analytical approach that produced it.

Rating Scope and Format

The format for risk ratings merits close attention because very few documents provide risk information other than ratings and because, as we noted earlier in this chapter, the most useful format would combine a narrative description of technical problems with a qualitative or quantitative rating.

For this part of the analysis, we expanded our concept of scope. In the preceding discussion, we focused on whether milestone documents and briefing materials cited the scope of the risk effort—all or selected subsystems or the system as a whole. We found that very few did, although risk ratings were reported in the majority of available documents and in about half of the available briefing materials. Thus, even if the scope of the effort was not cited, we can still ask: What was the scope of the ratings? We noted earlier that risk efforts are generally more useful when they cover all subsystems, not just selected subsystems or the system as a whole. Combining these two concerns, we cross-classified milestone documents and briefing materials by their format and scope to see in more detail how risk was rated for milestone reviews.

Few documents (15 percent) provided descriptions of technical problems along with a risk rating, and the documents that did covered the system as a whole or selected subsystems. None covered all subsystems. Of the briefing materials, 20 percent provided descriptions along with qualitative ratings, and half of these (10 percent) covered all subsystems. (See table 3.5.)

Table 3.5: The Format and Scope of Risk Ratings in Milestone Documents and Briefing Charts

	Format		
Scope	Descriptive	Qualitative	Both
Milestone documents			
System as a whole	7%	22%	10%
Selected subsystems	41	12	5
All subsystems	0	2	0
Briefing charts			
System as a whole	0	40	0
Selected subsystems	20	20	10
All subsystems	0	0	10

Summary

No program management office has quantified and budgeted for technical risks as called for by Initiative 11. Although the program offices for all 25 systems have made an effort to identify their technical risks, only 3 conducted risk efforts that meet our criteria for technical risk assessment.

In addition, we found wide variation in how risk efforts were implemented. The implementation of an effort depends partly on program circumstances, so we cannot expect all efforts to have been carried out in exactly the same way and cannot be certain that those we examined reflected inappropriate implementation decisions. But most of the offices did not consider the complexity or maturity of their systems when choosing implementation options regarding format, scope, and data collection procedures. Therefore, it is not likely that the efforts they implemented were as useful as they could have been for the further development of their systems.

The services and the DSARC must make decisions regarding the pace and direction of these programs during milestone reviews. Most milestone documents provided some information on technical risk, but this information rarely combined narrative information with ratings for all subsystems. Our analysis of briefing materials suggests that the program management offices were unlikely to add further details orally. Only about half of all such materials cited technical risk, and the materials that did rarely combined narrative information with risk ratings and rarely covered all subsystems.

BLANK PAGE

Chapter 4

Difficulties with Current Approaches to the Assessment of Technical Risk

When we collected our data, some issues arose that are not covered in our study's six initial evaluation questions. In this chapter, we discuss these issues. They concern program offices' working definitions of technical risk and risk rating categories, the provision of risk information to decisionmakers, DOD's training in technical risk assessment, and the risk information contractors provide to program offices.

Definitions of Risk and Risk Rating Categories

It is important that technical risk be clearly and consistently conceptualized within and across the program management offices. It is also important that risk rating categories be consistently defined. This is true regardless of the rating format—narrative, qualitative, or quantitative. Not all program offices need use the same format. But it is necessary that all those that use a qualitative format, for example, define high, moderate, and low risk in a similar way.

If definitions or rating formats are inconsistent, the decisionmakers will need to ask for clarification, and this could take considerable time. For example, if subsystem risks are not rated in terms that are familiar to reviewers, program staff may be required to revise the ratings or conduct an entirely new assessment. Worse yet is that inconsistencies may never be recognized and that program office managers (that is, the chief engineer, contract officer, and program manager) may base daily decisions on technical information that is vague and quite possibly misleading. This would also affect reviewers at higher levels in the services and the DSARC, where major "go-ahead" decisions are made.

Definitions of Technical Risk

We found that only 5 program management offices had a standard definition of technical risk set by office policy and known and applied by all staff members. Moreover, respondents in only 3 offices cited either DOD or service definitions of technical risk (perhaps in part because these definitions are ambiguous, as we discussed in chapter 2). Respondents in only one Air Force office were aware that Air Force Regulation 70-15 defines risk.

If neither documented DOD definitions nor program management policies have established a standard definition of risk, what definitions did the respondents actually use, standard or not, in their day-to-day work? Table 4.1 summarizes the answer.

Table 4.1: The Definitions of Technical Risk Used in the Program Management Offices

Definition	Number of offices
Likelihood of problems can be calculated	3
Probability of failure can be calculated	3
Probability of failure can be calculated, given schedule or cost limits	2
Technology is unproven or beyond the state of the art	2
Technical risk is too subjective to define	2
Probability of failure and the consequences can be calculated	0
Offices giving inconsistent definitions	4
Offices giving no definition	9

We entered definitions in the table if all or most respondents provided the same definition or if documentation provided one. No office cited the Defense Systems Management College definition that was based on the probability and consequences of failure (quoted in chapter 2), although 5 offices based their definitions on the probability, but not the consequences, of failure. In 2 of these 5, respondents defined technical risk as the probability of failure, given limited time or limited funding. In 3 more offices, respondents defined technical risk as the probability of failure but did not cite schedule or cost limits.

Other offices offered definitions that were similar to these but not based explicitly on the probability of failure. Two offices based their definitions on the degree to which the required technology was unproven or beyond the state of the art (not yet even partially developed). And 3 offices defined risk as the existence of a technical problem, or the likelihood that one would arise, but not necessarily a problem that would cause program failure.

In 4 offices, the definitions we were given were inconsistent in ways that could not be resolved by taking a definition from the majority of the respondents or from their program documentation. In 2 other offices, the majority of the respondents said simply that technical risk is too subjective to define. (Information was not sufficient for coding the 9 other offices.)

Definitions of Risk Rating Categories

As we noted in chapter 3, most program management offices rated risk in qualitative terms—high, moderate, and low (or red, yellow, and green). In our interviews, we asked respondents how they defined these qualitative terms. Their answers were not consistent.

Seven offices defined qualitative ratings in narrative terms. For example, high risk was sometimes defined as "solvable if the schedule or performance requirements are changed," moderate risk as "solvable with no changes" (or solvable without reducing the performance requirements), and low risk as "no problem." Three offices defined qualitative ratings by assigning probability ranges. For example, an 80-percent chance of not meeting performance requirements was high risk, a chance of 21-79 percent was moderate, and a chance lower than 21 percent was low. Two other offices used both narrative and quantitative terms.

In 3 offices, respondents did not agree on what rating format had been used, and the inconsistency could not be resolved by taking the majority's answer or referring to program documents. Five offices used qualitative ratings but said the terms are too subjective to define.

Neither narrative nor quantitative terms are necessarily preferable for defining qualitative ratings. Hence, this variation among the offices is not a problem. But when we examined the meanings attributed to narrative and quantitative terms, we found inconsistency persisting both within and across the offices.

Narrative Terms for Defining Qualitative Ratings

Respondents provided several versions of narrative terms for their qualitative ratings. In some cases, respondents in one office provided more than one narrative definition for high, moderate, or low risk. Some definitions were merely distinctive; others were contradictory. Table 4.2 summarizes them.

Table 4.2: Qualitative Risk Ratings in Narrative Terms Used in the Program Management Offices

Rating and term	Number of offices
High (red)	
Solvable with changes in schedule or performance specifications	6
Beyond the state of the art	4
Probable failure	2
Major problem	1
Test plan not yet devised	1
Current state of the art	1
No definition obtained from office	10
Moderate (yellow)	
Some development success but still uncertain	6
Solvable with no changes in schedule or specifications	2
Test plan devised but testing not yet completed	2
Caution	2
Beyond the state of the art	1
Solvable	1
No definition obtained from office	11
Low (green)	
Proven technology and no problems	9
Solvable	4
Test plan devised and tests completed	1
Solvable with no major schedule change	1
No definition obtained from office	10

High Risk

In some offices, narrative terms for high risk specified a problem as solvable if the schedule could be stretched or performance requirements could be made less stringent. In other offices, high-risk elements were considered probably, but not necessarily, unsolvable. In still others, high-risk elements posed "major problems," but the source of difficulty—cost, schedule, or performance—was not cited or tied to solvability. One office considered elements high in risk if they were currently within the state of the art, but 4 other offices said high-risk elements were beyond the state of the art. Finally, 1 office described risk as high if a plan for testing or managing development had not yet been devised. Early in the acquisition cycle, test plans may have been devised for elements that were neither within the state of the art nor entirely new. Testing is a criterion distinct from the criteria reported in other offices.

Moderate Risk

The terms for defining moderate risk were also inconsistent. Many offices used this rating to mean that uncertainty remained despite some success in development. But 1 office applied the rating to elements still beyond the state of the art. One office considered problems to have been moderate in risk if they were solvable, without stipulating anything about schedule delays. Two other offices added that schedules could not slip. Two offices used tests as the basis for rating risk.

Low Risk

There was more consistency in the definitions of low risk. Many offices cited proven technology, no problems, or no special technology required. But 5 offices said problematic elements could still be low in risk, provided there was no threat, or no major threat, to schedule. And 1 office used tests as the basis for qualitative risk ratings.

In several cases, definitions were inconsistent across the rating categories. For example, "beyond the state of the art" was used to describe moderate risk in 1 office but high risk in 4 others. "Solvable" was the definition of moderate risk given by 1 office but 4 others defined low risk in this way. Moreover, staff members in 3 program offices provided definitions that were inconsistent within categories. In 1 office, a respondent said high-risk technology was unproven, while another said high-risk technology may be within the current state of the art (already proven in at least other applications). In another office, one respondent based a definition of moderate risk on some development success. Another stipulated that moderate risk meant "beyond the state of the art"—that is, the technology had not yet been developed. In a third office, respondents defined low risk in contradictory terms, one citing no problems and another allowing problems so long as they were solvable.

These inconsistencies within and across rating categories imply that high, medium, and low are not adequate descriptions of risk. Yet, as we described in chapter 3, many offices used these ratings in their program documents, including those on which milestone review decisions were based.

In summary, we found widespread inconsistency in the narrative terms used to define qualitative ratings. Across offices, different criteria define high, moderate, and low. Some respondents within and across the offices contradicted one another, as when one definition of moderate conflicted with another or one definition of "moderate" was the same as a definition of "high."

Probabilistic Terms for Defining Qualitative Ratings

Most of the program management offices used narrative terms to define their qualitative ratings, but 5 used quantitative terms—that is, they used a probabilistic estimate to express the likelihood of not meeting performance requirements. We asked respondents who used quantitative terms to specify the range of probabilities they used to represent high, moderate, and low. Their answers were scattered across the range of probability from zero to 100 percent. The lower boundary for high risk ranged from 10 to 80 percent. That is, according to a respondent in 1 office, a chance of 10 percent or more that specifications would not be met was considered high risk. In another office, risk was not high unless the probability was at least 80 percent. For moderate risk, the probability ranged from as low as 3 percent to as high as 79 percent. For low risk, the upper boundary varied from 2 to 30 percent. Finally, respondents within 3 of these 5 offices cited inconsistent quantitative terms for risk.

In summary, inconsistency was widespread within and across offices that based qualitative ratings on probabilistic estimates of risk. Since no offices reported having used quantitative terms in the review process or in program documentation, reviewers may have seen only the qualitative ratings and may never have discovered or resolved the underlying discrepancies.

The only clear difference in the procedures the services used for rating risk concerns probabilistic terms. Comparing the 5 offices using these terms, 3 Army and 2 Air Force offices, we found that the Air Force set more stringent boundaries for high and moderate risk than the Army. For instance, a 60-percent chance of not meeting performance requirements would be rated high in risk in both of the Air Force offices but moderate in 2 of the 3 Army offices.

Program Management Staff Views on the Value of Qualitative and Quantitative Risk Efforts

In addition to obtaining the data on how the program management offices defined and rated risk, we asked staff, when it was appropriate, for their views on the value of qualitative and quantitative risk efforts. We expected the preferences of staff members to reflect the type of risk efforts performed in their offices, and this was indeed what we found. In this survey, few respondents (19 percent of the 53 who were asked this question) preferred quantitative ratings of risk, and not many (24 percent) thought the offices should be required to perform quantitative assessments. In line with technical risk efforts in their offices, more than half the respondents (60 percent) said they preferred either a qualitative or some other less structured procedure.

The reasons for these rating preferences warrant consideration, because they reveal characteristics of the various approaches that were perceived to be important. The reasons also suggest that further training in or support for technical risk assessment might be helpful. Respondents in several offices noted that quantitative ratings seem more rigorous, adding discipline to the assessment process or helping define program structure. Some respondents suggested that the results of quantitative efforts are more reliable, meaning that they more accurately identify risks. But many others said that it is difficult to express risk in quantitative terms or to apply one quantitative model across several different programs. Many said that quantitative efforts require resources (staff or time) not always readily available. And some claimed that the results of quantitative efforts are not reliable because they cannot be depended on to identify risks. Overall, the respondents in the 25 offices were twice as likely to cite the disadvantages of quantitative risk efforts as to cite any advantages. (See table 4.3.)

Table 4.3: Advantages and Disadvantages of Quantitative Risk Efforts Cited by the Program Management Offices

Opinion	Number of offices
Advantages	
Add rigor	9
Help define program structure	3
Are reliable	3
Help in estimating program costs	1
Conform to standard engineering approach to risk	1
Help support program decisions	1
Allow flexibility in rating risk	1
Disadvantages	
Require resources not always available	12
Use terms hard to define	9
Require application of the same model to different programs	6
Are not reliable	5
Reduce decisionmakers' flexibility	5
Do not produce timely results	2
Lead to micromanagement	1

When we asked the program management staff about qualitative ratings, the primary advantage they cited was the reliability of the results. Respondents in 2 offices noted also that the results from qualitative efforts are more timely than those from quantitative efforts. The primary disadvantage, according to others, is that qualitative results are not reliable—they are too subjective or imprecise. Even so, across the 25 offices, respondents were twice as likely to cite advantages of qualitative efforts, reversing the pattern for quantitative efforts. (See table 4.4.)

Table 4.4: Advantages and Disadvantages of Qualitative Risk Efforts Cited by the Program Management Offices

Opinion	Number of offices
Advantages	
Are reliable	6
Produce timely results	2
Correspond to conventional risk concepts	1
Are comprehensive	1
Produce results that are easy to communicate	1
Use resources that are available	1
Are acceptable to staff	1
Disadvantages	
Are not reliable	4
Require resources not always available	1
Do not produce timely results	1
Are not comprehensive	1

These differences in perceptions are not in themselves problematic, but they do suggest that the availability of various approaches to technical risk assessment (in the handbook of the Defense Systems Management College on risk assessment, for example) is not enough to ensure that program offices will adopt any particular approach or rely on the results.

Summary of Definitions

Few of the program management offices knew how DOD or service documents define technical risk, and few had their own policy formally defining technical risk. Many offices nonetheless had a definition shared informally by all or most staff members within an office, but the definitions varied widely from office to office. Some were predicated on the likelihood that technical problems would arise, others on the likelihood that problems would arise and lead to program failure. Some considered the likelihood of failure within cost or schedule constraints; others did not. Finally, in six instances, there were no consistent definitions of technical risk even within an office. Since few of the offices were aware of any DOD or service definition of technical risk, and since the definitions that do exist are ambiguous, the inconsistency we found in working definitions is not surprising.

Many offices expressed risk in qualitative ratings—high, moderate, and low or red, yellow, and green—and these ratings were defined in narrative or quantitative terms. For example, high risk was sometimes defined narratively, as in "beyond the state of the art," or quantitatively, as in "at least an 80-percent chance of failure." Within 3 offices, quantitative definitions were inconsistent; our respondents set different boundaries for the same levels of risk. But narrative as well as quantitative definitions were widely divergent across all offices and were often contradictory.

With definitions and ratings so inconsistent, confusion is almost inevitable. For example, one staff member may say that risk is high because the technology is unproven. Another may say risk is low because, although the technology is unproven, no serious problem is expected as long as time and funding are available. Still another staff member might see risk as moderate because no serious problem is expected but would also say that failure of any element would stop program progress. Moreover, where quantitative terms are used, a 30-percent chance of not meeting specifications is called low, moderate, or high risk, depending on which office makes the rating.

The results of a risk effort performed without regard for such inconsistencies will not be very valuable and may mislead decisionmakers. For example, program staff may believe that a 30-percent risk is low, while decisionmakers see a 30-percent risk as high. If review documents simply report low risk (none of those we examined had quantitative ratings), decisionmakers may never know that the estimate of risk was actually an estimate of 30 percent. Even if inconsistencies are later uncovered and resolved, time will have been lost. Furthermore, although respondents within many offices did use consistent definitions of risk and risk ratings, the inconsistency across them makes it very difficult for reviewers outside any office to evaluate the results of risk efforts or to compare results across programs.

The Communication of Information to Decisionmakers

In the following discussion, we approach the problem of communicating technical risk information from the separate perspectives of the offices and the reviewers. We examine the specific issues of access to information and its adequacy, content, and overall presentation.

The Program Management Office

All offices reported using their risk efforts in program management. In 23 offices (92 percent), we were told that risk efforts had been used to support technical decisions such as selecting design alternatives, program scheduling and restructuring, and assigning tasks to groups outside the program office. Seven offices (28 percent) also cited the use of risk efforts to support decisions on overall program cost or applications for funds to cover problems identified by their risk efforts. Finally, 1 office reported using its risk effort in the evaluation of vendors' proposals, having applied it also to technical decisions. The staff members we interviewed—program manager, deputy program manager, chief engineer, and contract officer—played key roles in the daily operations of a program. If technical risk information is to be used in the program decisions described above, these individuals must be aware of and have access to this information. In addition, they must have enough knowledge about risk efforts to understand the results and their limitations.

The importance of the program manager in both the program office and higher review processes makes this individual's knowledge about technical risks of particular concern. At the program office level, program managers have primary responsibility for daily decisions and are in a position to request a risk effort and ensure that their technical staff know about it. When preparing program documents and when briefing decisionmakers at program reviews, a program manager must address the question of risk.

Thus, in our interviews with program managers, we asked not only whether they were aware of the risk efforts performed for their programs but also whether or not the program managers knew how an effort had been performed. Specifically, we asked the program managers whether they knew

- format: Were risks rated in qualitative, quantitative, or narrative terms?
- scope: Was the focus on the system as a whole or on subsystems?
- procedure: Was input obtained from one individual or a group?
- sources of data: Did having technical risk information depend on the contractor, laboratory, program office, or other sources?
- approach: Were quantitative or qualitative approaches (such as those described in chapter 2) used to determine risk?

Having this knowledge would help program managers understand and evaluate the results of the risk effort and enable them to make well-informed reports to reviewers.

We found that the program managers were aware of the primary risk efforts for their programs, and most knew the format, scope, procedure, sources of data, and approach. But of the 25 managers we surveyed, some did not have complete information. For example, 5 managers did not know the approach that had been used to assess risk, and of these, 1 also did not know the format for reporting risk, 1 did not know the procedure for collecting technical risk information, and 2 did not know the sources of data. Two other managers knew the approach but did not know other aspects of how risk had been assessed; 1 did not know the scope and 1 knew neither the format nor the procedure. Such information is often important in managing and appraising the status of high-technology systems. Program managers who lack this information are therefore able neither to fully evaluate the results of their risk assessments nor to describe their assessments fully and promptly in the review process.

Although our analysis of interview data from other technical staff members was not as detailed as our analysis of data from the managers, the results reveal that some individuals had little or no information about risk efforts in the program management offices. In 9 of our 25 offices, there was at least one person who did not mention a risk effort that was described by others in the office. Furthermore, some of the gaps and inconsistencies in our data indicate a lack of communication about the risk efforts. For example, at least one staff member in each of 4 offices did not know the format; in each of 4 offices, at least one did not know the scope; and in each of 5 offices, at least one did not know the procedure for the primary risk effort on the system the office was responsible for.

Our respondents could not be expected to know all the details of the risk efforts. However, the individuals we interviewed (among them deputy program managers and chief engineers) who are in charge of, or give input to, aspects of the development of systems should know at least what efforts have been performed and have access to relatively detailed information about them. Otherwise, it will be difficult to maintain clear priorities for the technical aspects of system development.

Because of the effect that technical risk can have on contract decisions, we interviewed the programs' contract officers in order to determine how they learn about technical risk. Two said they got no technical risk information, and the others said they learned about technical risk in briefings, program documents, or informal discussions with the program office. However, as we reported in chapter 3, not all program documents and briefings included technical risk information, and when they did, much remained uncertain, such as the scope of the ratings and what they mean. Informal discussions and meetings may not be more complete than this.

We found differences between the services in staff knowledge about risk efforts, a greater proportion of Army staff lacking knowledge than staff in the two other services. More program offices in the Army had staff members who did not cite a risk effort described by others, even when it had been documented. And more offices in the Army had staff members who did not know the format, scope, or procedure of their risk efforts.

The Higher Review Levels

Decisionmakers at higher review levels obtain information on technical risk from milestone briefings and documents provided by the program offices. Only about half the briefing charts we obtained from the program offices in our study even made reference to technical risk. All that did used ratings to do so, only one providing information on scope and another on approach. To obtain additional information about technical risk, a reviewer would have had to ask the program manager for it specifically. Yet, as we indicated earlier, program managers might not have been able to go into further detail about results.

In addition, we found two problems with reviewers' reliance on program documents for technical risk information. First, as described in chapter 3, many documents contained no discussion of risk or an incomplete one. For example, some program documents included an overall rating of a system's technical risk but no explanation as to what the scope of the rating was—that is, what part or parts of the system had been considered. The 1985 decision coordinating paper update for the Air Force NAVSTAR User Equipment program contained an overall rating of risk for the system without an explanation of which subsystems, if any, had been considered in this determination. Some program offices used a qualitative format for risk ratings in their documents but provided no narrative of what they meant—an example is the Navy's V-22 Osprey acquisition plan. A third example of incomplete discussion of risk is the listing of risk items only, with no explanation of how or why the items were chosen. Technical risk was presented in this form in the acquisition plan for the Navy's Submarine Advanced Combat System.

Second, the program documents we reviewed did not present technical risk information in any standard way. They variously presented risk in quantitative, qualitative, and narrative terms, used any scale, and gave as much or as little detail as the program offices chose. Five programs in our sample used different formats from document to document. For example, an early version of the acquisition plan for the Air Force Short-Range Attack Missile reported risk in qualitative terms, but an update of the same document used descriptive terms only. It is unclear whether the risks increased, diminished, or stayed the same.

In 4 programs, the number of categories used to rate technical risk changed. In one document, for example, the V-22 Osprey program used ratings of low, low-medium, medium, medium-high, and high to represent risks. In another document for the same program, the ratings were low, moderate, medium, and high. "Moderate" and "medium," two different points on this scale, were treated synonymously elsewhere. What was meant by each scale was not described, nor was it clear how to compare the two scales.

Further, for 5 of the 25 programs, ratings for one subsystem changed without explanation. In the Advanced Helicopter Improvement Program, for example, the transmission was rated as a moderate risk in the technical risk assessment report but as a low risk in the integrated program summary and in the acquisition plan. These documents were prepared for the same milestone review. For neither AHIP nor any of the 4 other systems was there a documented explanation for changing the ratings. Thus, the task of recognizing the change and requesting additional information had been left to the reviewers.

Changes in the way risks were presented in the documents may have resulted from a reluctance to identify serious problems. Some staff members said that raters often hesitate to report "red" or "high" risk to reviewers, preferring lower ratings even when they are not appropriate. Changing the risk ratings in program documentation and extending the rating scales may be ways of avoiding high-risk areas.

Summary of Communication

We found that the approach of program management offices to addressing technical risk offered no guarantee that information would be provided to decisionmakers within the offices or at the higher levels of review. Most program managers and technical staff, but not all, were aware of the characteristics of their risk efforts, including the format for reporting risk, the scope, the procedures for collecting technical data, the sources of technical information, and the approach.

Neither the program documentation nor the briefings we reviewed were adequate for informing program staff or reviewers about technical risks. In some briefings and documents, technical risk was not even addressed. In others, risks were treated minimally, as when a system was given a qualitative risk rating with no explanation. Complicating the reviewers' task, different documents addressed risk differently, rating scales changed, and ratings changed, all without explanation.

Decisionmakers within the program offices and at higher review levels cannot base decisions on the true technical risks of a system if they do not know about an assessment, nor can they do so when they are not given enough information to evaluate or understand it. Ultimately, risk efforts that decisionmakers cannot use will not be effective.

Program Management Office Staffing and Training

In our interviews with program offices, we asked who was involved in selecting and performing the risk efforts. We also interviewed staff in service schools to determine what training was available to support the program office staff involved in risk efforts. In the majority of the program offices, we found that staff were involved in both selecting and performing risk efforts but that service school training for the assessment of technical risk was minimal. These results are presented in detail below.

Selecting and Conducting Risk Efforts

In 12 program offices (48 percent), responsibility for selecting the analytical approach for a risk effort rested at least partly with the technical staff. In 6 offices (24 percent), the program manager was also involved. Respondents in 9 offices (36 percent) said that contractors, laboratory representatives, advisory panels, or others outside the office participated in the selection.

Once an effort had been selected, who actually did the work? In 18 offices (72 percent), it was technicians, engineers, or other staff. The program manager was directly involved in assessments for 7 offices (28 percent). In 3 offices (12 percent) support staff, such as cost or systems analysts, assisted in the efforts, and in 8 (32 percent), prime contractors or support contractors participated. Seven offices (28 percent) used input from laboratory staff or advisory panels.

As for differences in the services, we found that Army program managers were never involved in selecting or conducting risk efforts. Several Navy and Air Force program managers did participate, probably because many Navy and Air Force risk efforts were part of ongoing program management.

Technical Risk Assessment Training

Despite staff involvement in selecting and conducting risk efforts, technical risk assessment was given little attention in the services' training courses. If addressed at all, risk was broadly defined as "program risk," which may include technical, cost, schedule, management, or contractor risk. Even in the courses that addressed risk exclusively, technical risk was discussed only minimally, and none of the schools taught quantitative or qualitative approaches to technical risk assessment.

For the most part, the service schools used courses in other substantive areas to cover program risk. At the Air Force Institute of Technology, program risk was addressed in courses on reliability and maintainability. The Naval Postgraduate School included a discussion of risk in its courses on program management and contracts. Similarly, the Defense Systems Management College covered risk in its program management course, and the Army Logistics Management Center discussed risk in courses focusing on program management, cost analysis, and systems analysis.

Only the Army Logistics Management Center devoted courses specifically to program risk as part of the regular curriculum. Since the early 1970's, the Center has taught a 2-week course called "decision risk analysis" to engineers and systems analysts and "decision risk analysis for logisticians," also 2 weeks, to persons concerned with logistics. The Defense Systems Management College recently offered a 2-1/2 day seminar on risk management for program managers.

Definitions and the coverage of technical risk varied from school to school, even in the courses focusing on risk. Personnel at the Air Force Institute of Technology reported that risk is discussed in the courses but not actually defined and not broken into specific categories of risk, such as cost, schedule, or technical performance. The Naval Postgraduate School defined risks as "unknowns" and talked about risk either generally or in terms of cost. The Defense Systems Management College also defined risks as "unknowns" but broke risk into cost, schedule, and performance. In the actual coursework, however, discussion of risk returned to more general terms. Similarly, the Army Logistics Management Center defined risk as "the probability of not meeting cost, schedule, or performance goals" but treated risk more generally in the program management, cost, and systems analysis courses. Only in the

Center's decision risk analysis courses was the discussion of risk more specific, although it dealt mainly with costs and schedules.

None of the service schools discussed approaches for assessing technical risk: if it was mentioned at all, it was typically only described. We found two exceptions: at the Defense Systems Management College, issues associated with technical risk were discussed in one of the management courses and in the risk management seminar, and at the Army Logistics Management Center, technical risk was discussed in cost analysis courses as input to the TRACE estimate.

When we asked school staff members to rate their services' support for technical risk training, their ratings reflected the amount of risk assessment training each school offered. Ratings were high for the Army, which reportedly gave a "great deal of support" to the Center's efforts. "Little or no support" ratings were given to the Air Force for technical risk assessment training at the Institute of Technology and the Navy for training at the Postgraduate School. Moderate joint-service support was said to be given to technical risk assessment training efforts at the Defense Systems Management College.

Summary of Training

Data from the service schools suggest that technical risk assessment has received little attention in the curriculum. The Army was the only service that offered a course on program risk as part of its regular course offerings. In courses in which risk was mentioned, and even in courses devoted to risk, technical risk was not a focus and neither were approaches to technical risk assessment. The discussion covered either schedule risk or cost risk or, more typically, program risk in general.

Reliance on Prime Contractors

Prime contractors for the major systems were responsible for many of the technical risk efforts described by program offices. Of the 25 program offices in our study, 8 (32 percent) relied on their prime contractors for primary or other risk efforts. Of these 8 offices, 6 had required the effort in the original proposals for source selection and 1 had required it as a "contract deliverable." The reason for the other contractor effort was not specified.

Of the 17 programs that did not rely on prime contractors for their risk efforts, 12 nonetheless used technical risk information supplied by prime contractors as input to their own efforts. For example, the Navy program office for the Joint Tactical Information Distribution System used monthly documented risk reports from the prime contractor.

The Air Force relied more on contractors than the two other services did. This is not surprising, given that Air Force Regulation 70-15 on source selection calls for industry to address risk in proposals. Most of the 12 offices that used technical risk information from contractors in their own risk efforts were in the Navy and Air Force. Only 1 office in the Army used contractor information.

We observed three problems with contractor information on technical risk and risk efforts.

1. Contractors' input was not always well documented. Seven programs obtained information, which was not documented at all, through informal discussions with contractor staff. When there was documentation, it was not always clear how contractors obtained their information on technical risks. For example, the contractor provided technical reports to the Air Force JTIDS program office that included risk ratings of a subsystem but gave no explanation of how the ratings had been made. Hence, the program staff had no opportunity to evaluate the information.

2. The program managers in offices whose risk efforts were conducted by their prime contractors were limited in the knowledge they had about the efforts. Five of the 8 program managers in these offices could not describe, even in the most general terms, the analytical approach their contractors had used. This restricted their ability to understand the limitations of the assessments.

3. Some program staff reported bias in information from industry. Respondents in some offices stated that because of industry's interest in winning and maintaining contracts, it presented systems in the best light possible, particularly in risk efforts included in proposals. Program staff reported that some ratings were lower than they should be. In addition, they reported that contractors left some risks out and problems unidentified, because the contractors wanted to give the impression that they could build the systems. Consequently, the program offices that received technical risk information from contractors, especially information they received during source selection, did not believe that this information accurately described a system's technical risks.

Of course, it might not be only contractors that had an interest in underrating a system's technical risks. DOD in general, and program management offices in particular, might sometimes have been constrained by the same interest. But we are concerned here with the nature and usefulness of technical risk information supplied by contractors. To summarize, this information was not always well documented, leaving program offices little or no opportunity to gauge its accuracy or monitor changes in it as programs progressed. Given the reported bias in contractors' risk efforts, it is especially important that program offices be able to evaluate and monitor contractor information. Without this ability, they could become overly optimistic in making technical, schedule, and cost decisions.

Summary

In this chapter, we have identified four problems that stem from the services' current risk efforts. Definitions of technical risk and risk ratings were not consistent. Few program staff could cite a DOD or service definition of risk (we discussed available definitions in chapter 2), nor could they say that any definition was formally used in their offices. Many program offices used informal definitions of technical risk, but these varied considerably across the offices. In 6 of the 25 offices, the definition varied within the same office. Definitions of qualitative risk ratings, whether quantitative or narrative, also varied within and across program offices and were often contradictory as well.

Complete information on technical risk was not provided to decisionmakers at the program management levels or at the higher levels of review. While most program managers were aware of the characteristics of their risk efforts, some managers and other staff were not. The documentation and briefings describing technical risks did not present risk adequately for the use of managers and other reviewers.

Training in technical risk assessment was generally lacking. Where risk was discussed in the service schools, the focus was typically on program risk. Sometimes technical risk was minimally described, but approaches for technical risk assessment were not taught.

Reliance on contractors for technical risk information has made for several problems. Contractors often performed risk efforts and furnished risk information for the program offices, both formally (in requests for proposals and contracts) and informally. The program managers stated that these reports may have been biased because of incentives the contractors had to simplify or minimize problems. In most cases, the managers were given either minimal or no documentation with which to evaluate and monitor a contractor's technical risk information.

BLANK PAGE

Conclusions and Recommendations

Technical risks are an inherent part of major weapon system development, and failure to anticipate these risks can lead to cost and schedule problems as well as the failure of a system. The importance of assessing technical risk has long been recognized in DOD and, accordingly, guidelines and regulations calling for these assessments have been issued. One such guideline calls for budgeting for technical risk. DOD has also supported the use of technical risk assessments in major program decisions. Defense officials have told the Congress that only systems with low or moderate technical risk would receive funding.

In this report, we have reviewed the current state of technical risk assessment performed by the Department of Defense for major weapon systems and attempted to answer six evaluation questions on policies, procedures, and applications across the armed services. We sought to learn how technical risk was defined, how assessments were designed and conducted, what information was available to decisionmakers, and how the results were conveyed to program management office staff and milestone reviewers. Four issues arose from the findings of our investigation, relating to difficulties in the areas of the consistency of definitions of risk and rating procedures, information flow, training, and the involvement of contractors.

Conclusions

DOD has provided a handbook of quantitative risk assessment approaches developed by the Defense Systems Management College in response to Initiative 11. DOD has not, however, clearly specified its expectations for addressing technical risks, and even its terminology for conceptualizing risk is ambiguous. There is no standard definition of technical risk or of risk ratings.

Initiative 11 called for the Army, Navy, and Air Force to quantify technical risks and allocate funds to deal with them but has had a negligible effect on the ways the three services handle risk assessment. One Navy command tried a total risk assessing cost estimate pilot program. But the Army simply maintained its preexisting TRACE program, and the Air Force maintained its own cost estimation techniques. None of the services adapted TRACE or any other procedures for the purpose of quantifying and budgeting for technical risk.

All 25 program management offices we examined evaluated technical risks in some way. However, given the lack of clarity in DOD definitions of technical risk and requirements for technical risk assessment, risk efforts varied from office to office. Only 3 program management offices had risk efforts that we could classify as technical risk assessments; that is, their risk efforts were

- prospective, examining risks before problems occurred;
- planned, not an incidental part of program discussions;
- explicit in attention to technical risks;
- documented, so that the results of an assessment could be shared with decisionmakers and staff; and
- reported at least twice in each acquisition phase, in order to determine how risks changed.

As we have noted in the report, these criteria are not necessarily definitive, but we believe they represent a minimal standard of quality for risk efforts in DOD. Risk efforts in 3 program offices met these criteria, supporting our position that the criteria are relevant and attainable.

Turning from design to implementation, we found few risk efforts carried out in ways likely to produce the most accurate and useful results. Few provided narrative information as well as risk ratings, covered all subsystems, or collected data from independent raters. Since the selection of risk assessment format, scope, and input procedure depends partly on the maturity and complexity of weapon systems, there is no single correct way to implement a risk effort. But few program offices reported tailoring their risk efforts to the systems being developed.

Risk ratings were frequently reported in review documents and briefings, but the analytical approach and scope of the risk efforts that produced these ratings were almost never reported, and the ratings seldom provided information on both the content and the level of risk.

We have noted that our study was not designed to measure the effect of technical risk assessment on outcomes such as program restructuring or cost growth, but the likelihood of finding such effects is probably low. The response of the Army, Navy, and Air Force to Initiative 11 was minimal, and none of the 25 program offices in this study used a technical risk assessment to support risk budgeting. Moreover, very few risk efforts met the minimal criteria we developed for evaluating technical risk assessments, and few were implemented in ways that are, in general, likely to produce the most useful and accurate results. Thus, while DOD has encouraged the assessment of technical risk and proposed various analytical approaches, it has provided no guidelines to program management offices on how to perform technical risk assessment. Risk assessors were left on their own to decide how to carry out this important function. Their efforts to assess risk were poorly designed and implemented, and the information available to decisionmakers from program documents and briefings was inadequate.

Our review pointed to four additional problems. First, informal definitions of risk and risk rating categories were inconsistent. Some program management offices had developed their own definitions of technical risk but staff definitions varied widely, both within and across the offices. Many offices used qualitative ratings of technical risk (such as "high," "moderate," and "low"), but the meanings of these terms were inconsistent, or contradictory, when examined across the offices.

Second, technical risk information was not always adequately conveyed to decisionmakers and staff within the program offices and at higher levels of review. Some program management staff members were unaware of the risk efforts that had been carried out for their systems, and others lacked important information on the assessment procedures and results. Program documentation and briefings often did not provide sufficient background on assessment procedures or explain risk ratings.

Third, the training that is given in support of the performance of technical risk assessments is insufficient. The service schools cover technical risk assessment minimally, and students are not provided with the opportunity to practice and compare applications of different assessment techniques.

Fourth, the programs often relied on contractors to identify technical risks but received inadequate information on the contractors' risk efforts. The program management offices usually received only the contractors' risk ratings and did not know how the risk efforts had been conducted or how the ratings were defined. Program management staff also believed that the risk efforts of contractors may have been biased because industry did not want estimates of extreme risk to jeopardize winning and maintaining contracts. (The same bias may have affected estimates of risk within the program offices or DOD, because Defense officials reportedly prefer to fund systems with only low or moderate technical risk.) The program offices did not receive sufficient information, in most instances, to evaluate the adequacy or accuracy of the contractors' risk efforts.

Bias and error are always possible in risk assessment, regardless of who performs it. But bias and error can more easily be uncovered and corrected if key concepts in risk assessment are defined consistently and if assessment procedures and results are open to subsequent review.

Recommendations to the Secretary of Defense

We recommend that the secretary of Defense take the following actions to improve technical risk assessment concepts and procedures:

1. define technical risk and categories for rating risk;

2. require that risk efforts focus explicitly on technical risk and be prospective, planned, and repeated at least twice, early and late, in each acquisition phase;

3. require program management offices to document their risk assessment procedures and results;

4. establish guidelines regarding options for format for rating risks, scope, data collection, and assessment approaches;

5. require that the technical risk information that program offices or contractors provide for review include a description of format, scope, data collection, sources of risk information, and assessment approaches; and

6. provide more focused training in technical risk assessment.

Since a few program offices have already performed risk efforts that met our five criteria and since they have implemented their efforts in ways that are the most likely to generate useful results, it is clear that these recommendations can be followed without incurring new or significant costs. Moreover, DOD has asserted that technical risk assessments can significantly reduce cost growth in acquiring new weapon systems. Thus, it seems reasonable to expect substantial savings from improvements in the design and implementation of these assessments. Of course, our recommendations concern only one element of program management and, by themselves, cannot ensure timely and efficient development efforts.

Agency Comments and Our Response

DOD reviewed a draft of this report. DOD's comments and our complete response are in appendix III. DOD generally concurred with the principal findings but argued that the report overemphasizes technical problems as distinct from the cost and schedule components of overall program risk. DOD concurred fully or partially with all recommendations except the one calling for making additional information on risk assessment procedures available for review (GAO's fifth recommendation). DOD expressed reluctance to place further requirements on program management and argued that cost growth has declined to about 1 percent, rendering such requirements unnecessary.

We believe that the findings demonstrate a need for more clarity in, and attention to, technical risk assessment in DOD. The findings do not suggest that technical risk is more critical than cost risk or schedule risk or that DOD's attention to cost or schedule risk can be reduced. We have recommended more consistency in assessment concepts and procedures, but we also recognize the need for tailoring assessments to particular programs. Since most of DOD's assessments did not meet minimal standards of quality, it is unlikely that they have contributed to any reductions in cost growth.

BLANK PAGE

Appendix I

Program Descriptions

This appendix briefly describes each program, its intended purpose, and the effort to identify its technical risks. For some programs, efforts were formal and discrete tasks. For others, they were informally part of program office routine. Many risk efforts were, in some respects, extensive and carefully done. Seven of them met four of the criteria we developed for this evaluation. But only three risk efforts—for the Antisubmarine Warfare Standoff Weapon, Remotely Piloted Vehicle, and Short-Range Air Defense Command and Control System—met all five essential criteria. Risk efforts for all programs are evaluated in terms of the criteria in table 3.1.

AHIP

The Army Helicopter Improvement Program (AHIP) seeks to upgrade the capabilities of the light observation helicopter fleet. The development effort, contracted to Bell Helicopter Textron, covers 14 subsystems, among which are a target observation and acquisition device above the rotor (a mast-mounted sight), the tail rotor drive shaft, and navigation and communication equipment. AHIP is slated to handle reconnaissance, security, and target designation and handoff in support of attack helicopters, air cavalry, and field artillery. It is expected to operate day and night, in hot weather, and at nap-of-the-earth altitudes.

The Army expressed interest in an advanced scout helicopter in 1974 but decided 5 years later that an entirely new helicopter was not affordable. In 1980, the Army began planning for a scout helicopter that would bolster the capabilities of an existing model. Full-scale engineering development for AHIP started in 1981, under the direction of the Aviation Systems Command in St. Louis, Missouri. Formal DOD review for milestone II was in early 1982.

In 1981, a decision risk analysis was performed, in preparation for source selection for the development contract. In personal interviews and a written questionnaire, technical and engineering staff rated risk for each AHIP subsystem on a six-point scale defined in qualitative terms ranging from "none or very low" risk to "unacceptably high" risk. The questionnaire provided a verbal description of each point on the scale and of lower and upper boundaries for the probability of not meeting performance requirements. For example, "unacceptably high" was described as "conceptualized on paper but still theoretical and may exceed current state of the art." In quantitative terms, risk was "unacceptably high" if the probability of not meeting requirements exceeded 50 percent. A support staff member summarized the ratings and then used them as input for a computerized schedule risk analysis, which generated various estimates of time to completion, such as "50-percent chance of completion within 37 months, 90-percent within 39 months."

ALWT

The Navy Mark 50 Advanced Lightweight Torpedo (ALWT) is an antisubmarine torpedo designed to enhance capabilities for target acquisition, speed, lethality, and depth. Its sonar system is intended to detect targets faster and in greater volumes of water than earlier torpedos could. Its engine is intended to render the torpedo faster, quieter, and able to dive deeper than conventional engines.

Under the Naval Sea Systems Command in Crystal City, Virginia, and under contract to Honeywell, the ALWT passed milestone II for full-scale development in early 1984. It is set for a production decision (milestone III) in late 1986.

The ALWT is a pilot program for the Naval Material Command risk management system called "solving the risk equation in transitioning from development to production." The program office has organized its risk management to conform to the command's guidelines. Extensive monthly and bimonthly reports from the contractor have provided current program data, such as test results showing the "mean time between failure" for various ALWT components. Results have been aggregated in various ways to reflect technical risk, and high-risk components have been discussed in meetings between program office staff and the contractor.

Some members of the staff decided to supplement the command's guidelines with an additional measure of risk not based on test results. Their measure, updated monthly, rates risk for each ALWT subsystem on a one-to-five scale. It has been included in the contractor's reports.

AMRAAM

The Air Force Advanced Medium-Range Air-to-Air Missile (AMRAAM) is an all-weather, radar-guided missile designed for Air Force and Navy fighter aircraft. Compared to missiles currently in production, AMRAAM will reportedly be less dependent on its launching platform for target designation and guidance. It will be guided by the aircraft radar until midcourse, when it will switch to its own radar. This "launch and leave" capability is intended to allow the pilot to break away after firing and engage other targets. Under development by Hughes Aircraft, AMRAAM is being designed also for greater speed, reliability, and resistance to electronic countermeasures than missiles now produced.

Under the Joint Systems Program Office, Armament Division, at Eglin Air Force Base, Florida, AMRAAM passed milestone II for full-scale development in 1982.

The primary risk effort was handled by ongoing program activities such as regular meetings of the program management staff and contractor to discuss test results and identify the program's "technical drivers." This approach led to efforts to reduce risk that were reflected in contract specifications, competition between contractors during the demonstration and validation phase, and program restructuring.

Other risk-related activities for AMRAAM are contractor reports, cost and schedule analyses, and a recent study of the overall program by a blue ribbon panel of Air Force and Navy reviewers.

ASAT

The Air Force Antisatellite Weapon (ASAT) is designed to destroy specified low-altitude satellites. The ASAT weapon comprises a two-stage missile and a miniature homing vehicle. The ASAT is to be launched from an F-15 fighter plane into space, where the miniature homing vehicle would maneuver into a satellite's orbit and destroy it by direct impact.

The ASAT is being developed by the Air Force Space Division in El Segundo, California. Boeing Aerospace Company is the contractor responsible for the missile and system integration; the miniature vehicle is being built by LTV Aerospace and Defense Company. The system has been under accelerated development and, when we finished data collection, had not yet had any formal DSARC milestone reviews.

The primary ASAT risk effort was performed by the program office to meet the information needs of authorities at higher levels. A probability of success for a system test was computed by combining probabilities of success for the performance of each subsystem. Qualitative ratings of the level of risk (high, medium, low) were assigned to each area of technical concern.

The program office also had additional information on technical risks, developed through informal assessments performed quarterly for the selected acquisition report and program review. These assessments relied on engineering judgment for subjective estimates of the technical risks of the system. Other risk information included formal cost risk estimates reported by the contractor for the miniature vehicle

ASPJ

The Airborne Self-Protection Jammer (ASPJ) is an electronic jammer used to provide tactical aircraft with the capability for defensive electronic countermeasures. It is designed to fit aboard a variety of aircraft, including the A-6, AV-8B, F-14, F-16, and F-18. The system is designed as five modules to allow different installation configurations to meet the requirements of individual aircraft.

The Navy is functioning as the lead service in this joint Navy and Air Force program. Management responsibilities are under the Naval Air Systems Command in Crystal City, Virginia. The program began full-scale development after passing milestone II in August 1979. The production decision, milestone III, is scheduled for 1986. The system has been jointly designed and developed by ITT Avionics and Westinghouse Defense, but the team members will be required to compete for the production phase of the program.

The program office has performed ongoing risk management and risk reduction efforts, reacting to problems as they arise. Test results have been relied on to reveal areas requiring attention.

Assessments of program cost, schedule, and technical risks were carried out by a support contractor when this program was part of the pilot total risk assessing cost estimate (TRACE) program. According to program personnel, the TRACE funding for the program was cut from the budget and the program is no longer part of the pilot effort.

ASW SOW

The Navy's Antisubmarine Warfare Standoff Weapon (ASW SOW) is a submarine-launched missile designed for quiet, buoyant ascent and short "time to target." It is a single-stage, rocket-propelled missile with two payload alternatives: the nuclear depth bomb and the advanced lightweight torpedo. It is intended as a tactical antisubmarine weapon for the SSN-637, SSN-688, and follow-on submarines. The program is run by the Naval Sea Systems Command in Crystal City, Virginia.

In February 1980, four companies were awarded contracts for a concept formulation study of the ASW SOW. From the results of these studies and the proposals each company submitted, Boeing Aerospace was chosen for the demonstration and validation work on the system. The program office received milestone I approval in December 1982 and plans milestone II for June 1986.

The primary ASW SOW risk effort was performed by Boeing. Technical risk was assessed as part of the risk management effort required in Boeing's contract. Boeing identified eight areas of technical risk and has continued to monitor these areas in the demonstration and validation phase. Three main activities were performed in order to identify risks. First, a "factory-to-target sequence" matrix was developed, laying out the acquisition steps from component fabrication to launch for each work breakdown structure element. Significant events in development and environmental considerations could be taken into account by using this matrix. Ratings of high, medium, and low were given to the elements with risk. Second, a risk element matrix was developed. mapping the work breakdown structure items against what Boeing calls risk elements of cost, schedule, performance, reliability and maintainability. production, and safety. Again, high, medium, and low ratings were assigned, as deemed appropriate. Third, because certain items tend consistently to cause problems in system development, data from other Boeing systems were used to identify risks. Boeing regularly reviews the system for potential risks other than the eight that were found from these three activities.

Risks are assessed and monitored by a risk management board, a small group of Boeing's ASW SOW management personnel. The Navy Sea Systems Command technical representative at Boeing is invited to the formal meetings and receives a copy of the minutes. The risk effort and the standards for rating risk have been documented in Boeing's risk management plan. Boeing has also documented the effect the risks are expected to have on the program and the steps that will be taken to abate them.

ATRS

The Navy Advanced Tactical Radar System (ATRS) is an anti-air-warfare system to be used in support of the defense of local areas. The Navy is still defining the ATRS concept, but, generally, it has been planned as a system that will have both a surveillance and a weapon support function. It is being designed for several platforms, including the next generation of surface ship combatants.

The ATRS had its genesis in 1982, and the operational requirements were documented in January 1984. Status as a major system was achieved in September 1984. The program, being developed under the Naval Sea Systems Command in Crystal City, Virginia, has remained unfunded during a reevaluation of the requirements. A milestone II review is expected late in fiscal year 1988 or early in fiscal year 1989.

A special group consisting of staff from the systems command, support laboratories, the program management office, and others is helping define the ATRS. The program manager has said that, because it is so early in the acquisition cycle, the risk effort has been limited to informal discussions of areas that may contain risk. The design options presented for the system were the impetus for these discussions. The program manager planned to use quantitative risk efforts for reporting to program management and reviewers.

C-17A

The C-17A Airlift Aircraft System will be designed to perform a full range of airlift missions in intertheater and intratheater roles, including air drops, combat offload, medical evacuation, and low and normal altitude parachute extraction of various types and sizes of cargo. It is intended to deliver cargo into small, austere airfields. The C-17A will be a turbofan wide-body aircraft powered by four engines being certified by the Federal Aviation Administration for commercial aircraft. It is intended to replace the active fleet of C-141B aircraft; it may also be used for roles currently filled by older C-130 aircraft.

The C-17A was initiated in 1979 (known then as the C-X) under the Aeronautical Systems Division at Wright-Patterson Air Force Base, Ohio. In July 1982, the Air Force awarded a contract to McDonnell Douglas Corporation for a modestly paced C-17 research and development program, and this received milestone II approval from the Air Force Systems Acquisition Review Council in 1981 and from the DSARC in November 1984. A milestone III review is planned for fiscal year 1987.

The risk effort has been carried out informally in the program office as a part of routine management, through technical interchange meetings held regularly with the contractor to discuss technical problems and issues. Each meeting has been structured around a particular functional area of the plane, so that different subsystems are examined at different meetings.

Technical risks for the system were also examined during source selection. Under Air Force Regulation 70-15, offerors were required to address technical risks in their proposals, and the source selection evaluation board considered the risks in selecting the winner.

CV-HELO

The CV Innerzone Antisubmarine Warfare Helicopter (CV-HELO) was initiated to provide a capability for fast-reaction, highly mobile, active sonar and torpedo delivery to assist in detecting, locating, and attacking enemy submarines entering the high-noise environment of the carrier battle group inner zone. It is intended to replace the SH-3H helicopter currently in service.

Developed under the guidance of Naval Air Systems Command in Crystal City, Virginia, the CV-HELO passed a milestone II review in January 1985. A contract for development was subsequently awarded to the Sikorsky Aircraft Company.

The program office has examined and reported technical risk issues in the program's monthly status report. Technical risks have been addressed subjectively in informal discussions with the program's engineering personnel.

HFAJ

The High Frequency Anti-Jammer (HFAJ) is being developed to provide anti-jam protection for tactical battle group operations. The HFAJ uses broadband frequency and has the ability to hop in the high-frequency spectrum. It is expected to provide a system with better availability, automation, and efficiency than the system currently used. The five parts of the system are the exciter, receiver, broadband power amplifier, anti-jam modem, and anti-jam controller.

In June 1981, the Chief of Naval Operations approved HFAJ development. The Navy subsequently awarded contracts to Rockwell-Collins, Westinghouse, and GTE for advanced development. The program office, under the Naval Electronic Systems Command in Crystal City, Virginia, was working toward a milestone II decision in 1984 when the secretary of the Navy stopped the funding. Since then, the system has been under review.

The primary HFAJ risk effort has been conducted by program management. At meetings, risk is discussed in an informal, subjective approach. Test results, work on other systems, personal experience, and the opinions of engineers and laboratory scientists, among other things, have been considered.

I-S/A AMPE

The Inter-Service/Agency Automated Message Processing Exchange (I-S/A AMPE) will handle secure and general-service command, control, communications, and intelligence for the armed services, other government agencies (such as the National Security Agency and Defense Intelligence

Agency), and U.S. allies. Overall, about 2,000 users are expected. It is being designed to modernize and standardize current hardware, software, and procedures.

The I-S/A AMPE program has undergone several shifts in concept definition since planning began in 1975. The Air Force became lead service in 1979 and assigned the program to its Automated Systems Program Office at Gunter Air Force Station, Alabama. I-S/A AMPE passed milestone I in 1983.

The primary I-S/A AMPE risk effort has been conducted as a set of management practices and decisions, including offeror conferences and surveys to evaluate design alternatives, review by service laboratories and expected users, independent validation and verification of technical plans, required certification by the National Security Agency of each system component, tests of critical components, and work plans that standardize the contractors' efforts and promote the integration of components.

As a result of activities like these, program management adopted a two-track development strategy. Track I is the development of low-risk items. Items not yet "reduced to practice" will be added later, if feasible, in track II "preplanned product improvement."

Two other management activities were a 1982 internal audit report that discussed technical issues and an independent cost analysis performed in 1983. A computerized system monitors the development schedule.

JSTARS

The Joint Surveillance and Target Attack Radar System (JSTARS) is designed as a surveillance, battle management, and target attack control system to detect, locate, and track targets. The JSTARS includes C-18 aircraft, airborne radar, airborne and ground data-processing and display equipment, secure anti-jam voice and data communication equipment, ground station modules, weapon interface units aboard fighter aircraft potentially able to carry missiles, and software support and development facilities.

The JSTARS was initiated as a joint Army and Air Force program, with the Air Force as the executive service, at Hanscom Air Force Base in Bedford, Massachusetts. The joint program, formed in May 1982, merged two programs: the Air Force Pave Mover, a system for detecting, locating, and striking mobile enemy armor, and the Army Standoff

Target Acquisition System, a radar system for fast, continuous, and broad helicopter surveillance of moving ground targets. Contracts were awarded to General Electric, Grumman, Hughes, and Westinghouse for studies of the radar and antenna.

Three risk activities were described by the respondents in our interviews in the program office. One was done solely on the antenna by Rome Air Development Center, the technical arm of the Air Force Electronic Systems Division at Hanscom. The group that assessed risk consisted of three engineers and a representative of Mitre Corporation, the system's engineering contractor. Contractors presented to this group the work they had done. Following the contractors' presentations, the group layed out a matrix describing what each contractor had done in the four areas that it judged would be a problem in developing the antenna and rated these areas as high, medium, or low risks. The group briefed the program director and Air Force officials on their results. The primary risk effort described in our report comprised these three activities.

The program management staff have also dealt with risk. Modeling, prototyping, technical studies, and engineering judgment have helped the staff make informal assessments for decisionmakers.

In accordance with Air Force Regulation 70-15, risk was also assessed by the source selection evaluation board. Before the proposals were reviewed, factors on which they were to be rated and standards for ratings were established. A separate high-medium-low rating scale was applied for technical risk.

JTIDS (Air Force)

The Joint Tactical Information Distribution System (JTIDS) is a time-divisional multiple-access communication system intended for jam-resistant digital communication of data and voice for command and control, positioning relative to navigation, and identification. The Air Force and Army JTIDS Class 2 terminals for the system are designed for fighter aircraft, ground tactical vehicles, and installations that have space and weight restrictions. The Class 2 terminal is composed of a receiver and transmitter unit developed by the Collins Government Avionics Division of Rockwell International and a data processor unit developed by the Kearfott Division of the Singer Company. Within the data processor are the interface unit, digital data processor, secure data unit, and battery.

Advanced development modeling of the Class 2 terminal in the late 1970's supported the use of JTIDS on platforms whose space is restricted.

The program was approved for full-scale development in January 1981. Milestone III production review is planned for May 1986. The Air Force, as lead service, runs the program from the Electronics Systems Division at Hanscom Air Force Base in Bedford, Massachusetts.

Two risk efforts were described in our program office interviews. The primary effort, which we reported in chapter 3, is an element in the management of the program. Discussions and meetings with Air Force staff, support contractors, and prime contractors are the main activity in this effort. The program management has also relied on experience with the JTIDS Class 1 terminal, designed for aircraft carriers and other major surface combat ships.

The second risk effort on the JTIDS was done for source selection before awarding a contract for full-scale development in 1981. The source selection evaluation board rated designated technical items for each bidder. Five color ratings, which the board defined in its instructions, were to be used for each item. An overall assessment of technical performance was rated high, medium, or low in a technical summary for each proposal, and the ratings and the overall technical summary were documented.

JTIDS (Navy)

The Navy Joint Tactical Information Distribution System (JTIDS) is intended to provide secure, jam-resistant communication, navigation, and identification by means of short pulses pseudorandomly distributed in time and frequency. The terminals for the system include a transmitter, a data processor, and receivers. The terminals are being developed in three classes—one for large surface ships (such as aircraft carriers) requiring high-power terminals and up to 10 voice channels, another for early-warning aircraft requiring up to 4 voice channels, and a third for tactical fighter aircraft and small surface ships requiring small, lightweight terminals with no more than 2 voice channels.

Work on the JTIDS began in 1974, with the Air Force as lead service. In 1976, the program split into two phases. One, directed by the Air Force, is to develop a time-division multiple-access system (which we discuss in the preceding section). The other, directed by the Navy, is to develop a distributed time-division multiple-access system that will allow simultaneous sending and receiving, operable with the Air Force system, which will not. Under the direction of the Naval Electronic Systems Command in Crystal City, Virginia, the Navy JTIDS is being developed by Hughes

Aircraft. It passed milestone II, into full-scale development, in 1982. Milestone III is not expected until 1992.

A cost and schedule risk analysis was performed by a support contractor in 1982, but the technical risk effort has been handled through program management efforts including, for example, testing and review by Navy laboratories and independent evaluation groups in DOD, review by potential offerors, and regular meetings of the program office staff and the contractor. Enhancements are to be added through "preplanned product improvement." Although the Navy JTIDS program was not among the pilot programs using the Naval Material Command risk management system, it reportedly followed a similar format in a 1984 technical review.

Mark XV IFF

The Mark XV Identification Friend or Foe (Mark XV IFF) combat identification system is intended to provide a reliable means of identifying airborne and surface targets at distances compatible with the ranges of "friendly" weapons. Currently, the target detection range capabilities and maximum ranges of many weapons exceed the ranges at which reliable identification is available. The Mark XV IFF is a question-and-answer system that will be introduced as a retrofit to the Mark X/XII IFF system, the transition to the new system to occur as platforms become available. The Mark XV IFF must be compatible with existing systems because it will have to operate in the same environment as these systems during the transition.

The program is a joint Air Force, Army, and Navy effort. The Air Force is the lead service for development, and management of the program is under the Combat Identification System Program Office of the Aeronautical Systems Division at Wright-Patterson Air Force Base, Ohio. The system is in the demonstration and validation phase of development. The milestone I review occurred in July 1984, and plans call for a milestone II review in fiscal year 1988. Both Texas Instruments and Bendix Corporation are under contract to perform the development work necessary before the system can enter full-scale development.

Several risk efforts have been carried out for the Mark XV IFF. The primary effort was an assessment conducted by the Air Force chief scientist as a result of questions arising in the review process. A panel was assembled to identify the areas of technical risk and assess the relative technical merits of alternatives.

Other Mark XV IFF risk efforts centered on the use of informal engineering judgments of problem areas in the system. The milestone I review and the decision on the type of development contract took risks into consideration.

MLRS/TGW

The Terminal Guidance Warhead (TGW) is one of three warheads being developed for the Multiple Launch Rocket System (MLRS). The MLRS is designed to deliver a large volume of fire power in support of field artillery. The TGW will enable the system to destroy armored vehicles and equipment. It is an autonomous warhead with terminal homing and fire-and-forget target capabilities.

The warhead MLRS/TGW is a multinational program. France, Great Britain, West Germany, and the United States are involved in the system's development. Each country has a representative in the program office, which is located at the Army's Missile Command in Huntsville, Alabama. The contractor is also multinational. Brandt Aremento (Thompson-Brandt) of France, Thorn EMI Electronics of Great Britain, Diehl G.M.B.H. of West Germany, and Martin Marietta of the United States formed MDTT Corporation for the development of the warhead.

A preliminary investigation of the technology began in the early 1970's. In 1977, the House Armed Services Committee required that it be developed as an option for the MLRS. About the same time, the secretary of Defense required that it be pursued as a multinational program. Following the signing of the memorandum of understanding between the four countries in 1979, work to define the TGW concept began. Passing milestone I in September 1984, the program moved into what is called the component demonstration phase. A milestone II review is planned for early 1987.

The primary risk effort focused exclusively on technical risk. It was made by the multinational group as part of its discussion of program options in the concept and international program definition phase. In about 1 week in informal discussion based on the experience of its members and prior work on TGW technology and other systems, the group identified 14 potential risk areas, screened the list, and rated the risks high, medium, and low. This led to a smaller list of 5 areas. The effort was exclusively for use in choosing the best alternative.

A schedule risk assessment was also performed for the TGW by a systems analyst at the missile command as part of the multinational effort in the definition phase. Although schedule risk was the emphasis, the analyst said that a technical assessment had to be made before the schedule work could be done. Information from the multinational group was collected and laid out in a network. Since a number of concepts were being considered, the assessment was made as generic as possible rather than dependent on a particular design choice. Another analyst added cost figures to the schedule assessment.

M1A1

The Army M1A1 program is intended to enhance the capabilities of the M1 Abrams tank. M1A1 development began with replacement of the M1's 105-millimeter cannon with a 120-millimeter version. The effort was expanded to develop armor for protecting the tank's mobility and firepower and an air distribution system for protecting it against nuclear, biological, and chemical warfare. Ammunition is to be developed and cannon components are to be built for the 120-millimeter gun to ensure its interchangeability with the West German Leopard 2 tank. Development is under contract with General Dynamics.

Under the Tank Automotive Command in Warren, Michigan, the M1 began prototype development in 1973 and entered full-scale engineering development 3 years later. During this phase, the 120-millimeter gun was incorporated into the development effort. The baseline M1 passed its milestone III production decision in 1979; the M1A1, including the gun and other enhancements, passed milestone III in 1984. Enhancements are to be phased into production over the next several years.

The primary M1A1 risk effort was a series of three TRACE analyses performed in 1982, 1983, and 1984. Staff members reportedly considered technical risk when they estimated cost inputs for the analyses and came up with estimates of high, low, and most likely cost for each M1A1 enhancement. TRACE was used to support applications for risk funds but not to guide technical decisions within the program office or at higher levels of review. Two other activities guided technical decisions: analyses of test results and informal staff discussions. According to the program manager, "ad hoc risk assessment, conscious or unconscious," has been part of the daily routine.

NAVSTAR User Equipment

The NAVSTAR User Equipment is part of the NAVSTAR Global Positioning System (GPS), a space-based radio navigation system consisting of satellites, satellite control and monitor stations, and equipment for their use. The GPS is designed to provide worldwide three-dimensional position and velocity and universal coordinated time information. The system can operate in all weather and has a high resistance to jamming.

The user equipment consists of a receiver and processor unit, an antenna system, a control display unit, a flexible modular interface, and an optional data loader. The equipment is designed to receive and process either simultaneous or sequential data from four different satellites. The user equipment measures velocity and range with respect to each satellite to derive the user's three-dimensional position and velocity. It then processes the data in terms of an earth-centered, earth-fixed coordinate system and displays the information in geographic or military grid coordinates. Magnavox Advanced Products and Systems Company and the Collins Government Avionics Division of Rockwell International are both under contract for the development of the user equipment. The two will compete for the production phase of the program, with the possibility of taking a leader-follower approach.

The system is a joint effort of the Air Force, Army, Navy, and Marine Corps, with the Air Force functioning as the lead service for development. The program management office is part of the Air Force Space Division in El Segundo, California. In the full-scale development phase, the user equipment was scheduled for a milestone III review in May 1986. The system passed a milestone II review in 1979.

The program office has considered the schedule and cost of technical problems as ongoing management of risks. Testing has been emphasized, and test results, reliability measures, and subjective judgment have been combined in order to identify technical risks. The program office also conducted an examination of technical risks in accordance with Air Force Regulation 70-15 for the source selection for production.

RPV

The Army Remotely Piloted Vehicle (RPV) has a long development history that began in 1975. Currently, it is being developed by Lockheed. Its high-technology subsystems include forward-looking infrared radar and an anti-jam capability. Developmental work on the RPV began in 1979, under the direction of the Army Aviation Systems Command in St. Louis, Missouri, but the RPV did not become a major system requiring milestone review until 1983. Its first milestone will be the production decision, at milestone III, in 1986.

A decision risk analysis, conducted in 1981 and updated in 1982, 1983, and 1984, covered schedule risk, assigning high, low, and most likely estimates of time required to complete development. The 1981 analysis and the 1982 update provided ratings of technical risk, basing them on a questionnaire completed by the technical staff. The RPV subsystems were rated on a scale that included qualitative labels and verbal descriptions of risk categories, plus probability ranges for the likelihood of failing to meet performance requirements. The scale differed slightly from year to year. In 1982, it ranged from "none or very low" risk (less than a 5-percent chance of not meeting requirements) to "unacceptably high" risk (greater than a 50-percent chance). In 1981, the scale ranged from "none or low" (not more than a 10-percent chance) to "unacceptably high" (greater than 50-percent, as in 1981). Questionnaire results were summed into a single rating (high, moderate, or low) for each subsystem.

Other risk-related activities for the RPV include a decision risk analysis completed in 1978 and TRACE analyses in 1982 and 1983 for the production phase.

SHORAD C2

The Short-Range Air Defense Command and Control System (SHORAD C2) offers automated command and control functions for the SHORAD batallion. Computers, display devices, software, and interface equipment are intended to automate the collection, processing, distribution, and display of information for SHORAD weapons. No existing system performs these functions; some of them can be performed manually, but this is slow and unreliable. The program office is at the Ballistic Missile Defense System Command in Huntsville, Alabama.

In July 1981, an acquisition strategy was approved by a general-officer review, which was supported by an Army in-process review in April 1982. However, the Congress accepted neither the schedule nor the funding requirements for the 1983 fiscal year appropriation. The Congress did acknowledge the need for an automated command and control system, and in response, the deputy undersecretary of Defense for command, control, communications, and intelligence approved a restructuring of the program in April 1983. Budget reductions led to another restructuring in the spring of 1984 and still another in early summer.

Three risk efforts have been completed for the SHORAD C2. The first, completed in January 1984 by a systems analyst at the missile command, focused on cost and schedule risk. Although technical risk was considered in the schedule and cost assessment, only the cost and schedule aspects were documented. The two other efforts were made in response to the program's restructuring. The second risk effort was completed in August 1984 and focused on the schedule risk of the software development. It was performed by a support contractor who borrowed heavily from the earlier effort. No mention was made of the technical risks of the system in the documentation.

The third effort, completed in March 1985, was the primary risk effort. It was made by a different support contractor, who used the systems engineering management guide published by the Defense Systems Management College. Probabilities of failure assigned to hardware and software components were based on their degree of maturity, complexity, and dependence on interfacing items. The probability assignments were subjective but based on standards documented in the engineering guide. Standards for high, medium, and low were also documented. The support contractor incorporated technical risk in the cost and schedule analyses.

SRAM II

The Short-Range Attack Missile II (SRAM II) is being developed to replace the current Short-Range Attack Missile and is intended to support penetrating bomber missions through the 1990's and beyond. The penetrating bomber mission is an essential element of the strategic triad of land-, sea-, and air-based defense. The SRAM II is intended to provide the B-1B and advanced technology bombers with a supersonic air-to-ground nuclear missile designed to attack fixed and relocatable targets. The system consists of the missile, support equipment, mission planning equipment, and carrier interfaces.

The SRAM II is being developed at Wright-Patterson Air Force Base, Ohio, in the Air Force Aeronautical Systems Division. The system start was approved in 1983. With an accelerated development approach, no milestone I review was held, and no discrete demonstration and validation phase has been conducted. Rather, a single "pre-full-scale" development effort is under way, with a milestone II review planned for 1986.

The program office has relied heavily for technical risk information on past work on similar systems. It has conducted an informal, subjective assessment of all subsystems but intends to reconsider this assessment approach for full-scale development.

SUBACS

The Submarine Advanced Combat System (SUBACS) is an integrated combat control system for the nuclear-powered SSN-751, SSN-752, and

SSN-753 submarines, now under construction. It is designed to merge sonar, sensors, fire control, and other control units into an integrated system. Originally a "preplanned product improvement" system, with two upgrades of the basic version for future submarines, the SUBACS has undergone a total restructuring because of problems in developing a revolutionary fiber optics data bus to connect the system's computers.

The SUBACS program is being developed by the Naval Sea Systems Command in Crystal City, Virginia. It was initiated in November 1980 with the approval of a mission element needs statement by the secretary of Defense. At milestone II review in September 1983, full-scale development was approved and, in December 1983, the Federal Systems Division of IBM received the contract award.

The risk effort reported in our interviews with staff in the program office was part of a schedule risk assessment performed by Naval Underwater Systems Command and IBM in response to a request in February 1983 from the assistant secretary of the Navy for a quantitative analysis of the risk to ship delivery dates. IBM and the Navy command worked independently to identify critical items, including items offering a "significant technical challenge," and these items served as the basis of a network analysis. Originally designed to be ongoing, the assessment was discontinued in December 1983.

T45TS

The multifaceted T-45 Training System (T45TS), or the Naval Undergraduate Jet Flight Training System, consists of aircraft, simulators, academic coursework, and training management. It is intended for the intermediate and advanced phases of the naval flight training program for jet aircraft pilots. The T-45 aircraft is a two-tandem-seat, jet-engine trainer designed and built in Great Britain. A version with the capability of operating from aircraft carriers will be built in the United States for the Navy by McDonnell Douglas Corporation.

Accelerated development of the system is under the guidance of the Naval Air Systems Command in Crystal City, Virginia. Combined milestone I and II reviews were made in October 1984, and the secretary of Defense approved full-scale development in December 1984. A milestone III review is scheduled for fiscal year 1988.

The program office has an ongoing risk management effort. Emphasizing reliability, the engineering staff has monitored risks by means of tests of problem areas. In addition to this effort, the program office was directed to use the template system of risk management detailed in "Solving the Risk Equation in Transitioning from Development to Production" (DOD 4245.7-M), which it did in the milestone I-II review.

Trident II (D5)

The Trident II (D5) Strategic Weapon System is intended to improve the performance of submarine-launched ballistic missiles. A follow-on to the Trident I (C4), the Trident II (D5) will reportedly provide a larger missile with greater accuracy and better payload. It is to be deployed on newly constructed SSBN-726 (OHIO) submarines and backfitted on other submarines of the same class that originally carried the Trident I (C4). The contractors involved in Trident II (D5) development include Draper Laboratories, General Electric, Interstate Electronics, Lockheed, Sperry, and Westinghouse.

The Navy's Strategic Systems Project Office in Crystal City, Virginia, manages the development, production, and support of the Trident II (D5) Strategic Weapon System, which began full-scale development after the milestone II review in September 1983. A milestone III review is scheduled for March 1987.

The program management office has used a risk management approach for addressing technical risk, examining low-risk technologies as much as possible. The office identifies problems through a steering group that includes senior contractor personnel in order to promote an exchange of information between the contractors.

An "improved accuracy program" was completed in 1982. This was a special assessment of the technology of critical elements in order to determine the feasibility of achieving the expected improvements in accuracy of the Trident II.

A separate schedule risk assessment was performed in 1983 by a support contractor. The assessment was aimed at determining schedule risks for the delivery of government-furnished equipment and information for submarines under construction.

V-22 Osprey

The V-22 Osprey program, formerly Joint Vertical Lift Aircraft (JVX) program, is an effort to develop, produce, and deploy a multimission vertical take-off and landing aircraft combining the capabilities of a turboprop aircraft with those of a helicopter. It uses a tilt rotor that allows vertical take-off and makes a transition to horizontal flight by means of tilting-engine nacelles.

It is a joint program of the Navy, Marine Corps, and Air Force and is to fulfill a different mission requirement for each service. The Navy is the lead service and fills the procurement role for the Marine Corps. The management of the program is under the Naval Air Systems Command in Crystal City, Virginia.

An initial operating capability that would replace the Marine Corps medium assault vertical lift fleet is planned for 1991. The program passed a milestone I review in December 1982, with Bell Helicopter Textron and Boeing-Vertol under a joint contract for development.

The program office uses an ongoing, informal process of risk assessment carried out by the engineering staff. As technical problems arise, they are discussed in routine staff meetings. Earlier, in an effort to determine the most feasible technical approach for the system, a joint technology assessment group examined risk as part of its evaluation of helicopter versus tilt-rotor designs.

Bibliography

AMDOR, Stephen L., and Roy R. Kilgore. "Quantitative Risk Assessment: A Test Case." Master's thesis, Air Force Institute of Technology, School of Systems and Logistics, Wright-Patterson Air Force Base, Ohio, 1974.

ANDERSON, Richard M. "Handling Risk in Defense Contracting." Harvard Business Review, 47 (July 1969), 90-98.

ARMY DEPARTMENT, Office of the Assistant Chief of Staff for Force Development (ed.). Proceedings, 12th Annual U.S. Army Operations Research Symposium, Washington, D.C., October 2-5, 1973, vol. 2. Washington, D.C.: 1973.

ARMY LOGISTICS Management Center. A Course of Instruction in Risk Analysis. Fort Lee, Va.: 1971.

BABIARZ, Anthony S., and Peter W. Giedras. "A Model to Predict Final Cost Growth in a Weapon System Development Program." Master's thesis, Air Force Institute of Technology, School of Systems and Logistics, Wright-Patterson Air Force Base, Ohio, 1975.

BAILLIE, Allan S. "Management of Risk and Uncertainty." Research Management, 23:2 (March 1980), 20-24.

BANASH, Robert C., and James B. Beeson. Cost/Schedule Uncertainty Analysis of the XM1/Alternative Programs. Rock Island, Ill.: Army Armament Command, Systems Analysis Directorate, 1976.

BARNETT, Paul J., and Harman K. Wales. "An Assessment of the Applicability of Production Readiness Reviews to Multinational Coproduction Programs." Master's thesis, Air Force Institute of Technology, School of Systems and Logistics, Wright-Patterson Air Force Base, Ohio, 1981.

BEECKLER, C. Eugene, and Kimrey D. Newlin. Economic Price Adjustment (EPA) Provisions. Fort Lee, Va.: Army Procurement Research Office, 1977.

BELL, Chauncey F. Cost-Effectiveness Analysis as a Management Tool. Santa Monica, Calif.: RAND Corp., October 1964.

BEVELHYMER, Herbert L. "A Proposed Methodology for Weapon System Development Risk Assessment." Master's thesis, Air Force Institute of Technology, School of Engineering, Wright-Patterson Air Force Base, Ohio, 1973.

BLANNING, Robert W., et al. Research Opportunities in the Management of Weapons Systems Acquisition. Philadelphia, Pa.: Wharton School of Finance and Commerce, Department of Decision Sciences, September-November 1975. Includes executive summary.

BLUE RIBBON Defense Panel. Report to the President and the Secretary of Defense on the Department of Defense. App. E. Staff Report on Major Weapon Systems Acquisition Process. Washington, D.C.: July 1970.

BOWERS, David G., and Stanley E. Seashore. "Predicting Organizational Effectiveness with a Four-Factor Theory of Leadership." Administrative Science Quarterly, 11 (1966), 238-63.

BRUNO, O. P., and Raymond Bell. "Analysis of Testing Risks for an Air Defense System." Proceedings, Annual Reliability and Maintainability Symposium, Washington, D.C., January 28-30, 1975, pp. 427-31. New York: Institute of Electrical and Electronics Engineers, 1975.

CARTER, R. D. A Survey of Techniques for Improving Cost Estimates of Future Weapon Systems. Falls Church, Va.: Analytic Services, March 1965.

CBO (Congressional Budget Office). A Review of the Department of Defense December 31, 1982 Selected Acquisition Reports (SARs). Washington, D.C.: August 1983.

COLVIN, Charles E. "Radar Hardware Second Buy Decision Risk Analysis." In Army Department (ed.), Proceedings, 12th Annual U.S. Army Operations Research Symposium, vol. 2, pp. 745-57. Washington, D.C.: 1973.

COREY, James M. "The Inefficiency of Sealed-Bid Competition." Defense Systems Management Review, 3:2 (Spring 1980), 42-46.

COX, Larry, and Michael Bohn. Acquisition Strategy Comparison Model (ASCM). Vol. 1. Executive Summary and Report. Arlington, Va.: Analytic Sciences Corp., May 1982.

-----. Acquisition Strategy Comparison Model (ASCM). Vol. 2. Appendices. Arlington, Va.: Analytic Sciences Corp., 1982.

CRAWFORD, Leslie P. "A Case Study in Risk/Decision Analysis." Student report, Defense Systems Management College, Fort Belvoir, Va., 1973.

CUFF, James D. "Risk-Decision Analysis in Weapons System Acquisitions." Long Range Planning, 6:1 (March 1973), 49-55.

CUMMINS, J. Michael. "Incentive Contracting for National Defense: A Problem of Optimal Risk Sharing." Bell Journal of Economics, 8:1 (Spring 1977), 168-85.

DAVIS, Guy W. "The Dilemma of Uncertainties Associated with Cost Estimating in the Project Management Office." Student paper, Defense Systems Management School, Fort Belvoir, Va., 1976.

DEFENSE SYSTEMS Management College. Risk Assessment Techniques: A Handbook for Program Management Personnel. Ft. Belvoir, Va.: 1983.

DEMONG, Richard F. "The Effectiveness of Incentive Contracts: What Research Tells Us." National Contract Management Quarterly Journal, 2:4 (December 1978), 12-22.

DIXON, Max Wayne. "A Statistical Analysis of Deviations from Target Cost in NAVAIRSYSCOMHQ Fixed-Price Incentive Contracts During the 1949-1965 Time Frame." Master's thesis, Naval Postgraduate School, Monterey, Calif., March 1973.

DOD (U.S. Department of Defense), Office of the Assistant Secretary of Defense, Comptroller. Acquisition Management: Selected Acquisition Report. Washington. D.C.: n.d.

-----, Office of the Assistant Secretary of Defense, Systems Analysis. Proceedings, Department of Defense Cost Research Symposium, Arlington, Va., March 2-3, 1966. Washington, D.C.: 1966.

"DOD Tests Contract Incentives." Defense Management Journal, 19:2 (1983), 43.

EBERTH, Robert William. "Escalation Provisions in DOD Procurement: A Review of the Problem and a Framework for Analysis." Master's thesis, Naval Postgraduate School, Monterey, Calif., 1974.

EDGAR, John D. "Controlling Murphy: How to Budget for Program Risk." Concepts: The Journal of Defense Systems Acquisition Management, 5:3 (Summer 1982), 60-73.

EMMELHAINZ, Margaret A. "Innovative Contractual Approaches to Controlling Life Cycle Costs." Defense Management Journal, 19:2 (1983), 36-42.

FALLOWS, James. National Defense. New York: Random House, 1981.

FINCH, Frederick E. "Collaborative Leadership in Work Settings." Journal of Applied Behavioral Science, 17:3 (1977), 292-302.

FISHER, G. H. The Nature of Uncertainty. Santa Monica, Calif.: RAND Corp., 1973.

FOX, Frank. Decision Risk Analysis: Army Helicopter Improvement Program/Near Term Scout Helicopter. St. Louis: Army Aviation Research and Development Command, 1981.

FOX, J. Ronald. Arming America: How the U.S. Buys Weapons. Cambridge, Mass.: Harvard University Press, 1974.

-----. "Note on Government Contracting and Methods of Government Procurement." Mimeo, Harvard Business School and Intercollegiate Case Clearing House, Boston, Mass., 1980.

GANSLER, Jacques S. "A New Dimension in the Acquisition Process." Defense Systems Management Review, 1:4 (Autumn 1977), 6-12.

-----. The Defense Industry. Cambridge, Mass.: MIT Press, 1980.

GAO (U.S. General Accounting Office). A Range of Cost Measuring Risk and Uncertainty in Major Programs—An Aid to Decisionmaking, PSAD-78-12. Washington, D.C.: February 2, 1978.

-----. Delays in Definitizing Letter Contracts Can Be Costly to the Government, PSAD-80-10. Washington, D.C.: November 16, 1979.

-----. Better Navy Management of Shipbuilding Contracts Could Save Millions of Dollars, PSAD-80-18. Washington, D.C.: January 10, 1980.

-----. Financial Status of Major Federal Acquisitions September 30, 1979, PSAD-80-25. Washington, D.C.: February 12, 1980.

-----. Issues Identified in 21 Recently Published Major Weapon System Reports, PSAD-80-43. Washington, D.C.: June 12, 1980.

-----. Use of Cost-Deferred-Fee Contracts Can Be Costly to the Government, MASAD-81-10. Washington, D.C.: March 11, 1981.

-----. Financial Status of Major Federal Acquisitions September 30, 1980, MASAD-81-13. Washington, D.C.: March 20, 1981.

-----. Acquiring Weapon Systems in a Period of Rising Expenditures: Implications for Defense Management, MASAD-81-26. Washington, D.C.: May 14, 1981.

-----. Improving the Weapon Systems Acquisition Process, MASAD-81-29. Washington, D.C.: May 15, 1981.

-----. The Navy Can Reduce the Cost of Ship Construction If It Enforces Provisions of the Contract Escalation Clause, PLRD-81-57. Washington, D.C.: August 24, 1981.

-----. Status of Major Acquisition as of September 30, 1981: Better Reporting Essential to Controlling Cost Growth, MASAD-82-24. Washington, D.C.: April 22, 1982.

-----. Improving the Effectiveness and Acquisition Management of Selected Weapon Systems: A Summary of Major Issues and Recommended Actions, MASAD-82-34. Washington, D.C.: May 14, 1982.

-----. Assessment of Admiral Rickover's Recommendations to Improve Defense Procurement, PLRD-83-37. Washington, D.C.: January 27, 1983.

-----. Status of Major Acquisitions as of September 30, 1982, NSIAD-83-32. Washington, D.C.: September 7, 1983.

-----. Weapon Systems Overview: A Summary of Recent GAO Reports, Observations, and Recommendations on Major Weapon Systems, NSIAD-83-7. Washington, D.C.: September 30, 1983.

GAO. The Army Needs More Comprehensive Evaluations to Make Effective Use of Its Weapon System Testing, NSIAD-84-40. Washington, D.C.: February 24, 1984.

-----. DOD Needs to Provide More Credible Weapon Systems Cost Estimates to the Congress, NSIAD-84-70. Washington, D.C.: May 24, 1984.

-----. Opportunities to Strengthen Planning for the Navy's Aircraft Engine Research and Technology Programs, NSIAD-85-13. Washington, D.C.: December 4, 1984.

GATES, Robert K., Robert S. Bicknell, and John E. Bortz. "Quantitative Models Used in the RIW Decision Process." Proceedings, Annual Reliability and Maintainability Symposium, Philadelphia, Pa., January 18-20, 1977, pp. 229-36. Washington, D.C.: 1977.

GERBER, Hans U. An Introduction to Mathematical Risk Theory. Philadelphia, Pa.: Wharton School, 1979.

GILBY, Howard M. "Decision Risk Analysis of the Impact of the Heavy Lift Helicopter Advanced Technology Component (ATC) Program of Alternative Methods of Powering the ATC Dynamic System Test Rig." In Army Department (ed.), Proceedings, 12th Annual U.S. Army Operations Research Symposium, vol. 2, pp. 572-82. Washington, D.C.: 1973.

GILMORE, David C., Terry A. Beehr, and David J. Richter. "Effects of Leader Behavior on Subordinate Performance and Satisfaction." Journal of Applied Psychology, 64:2 (1979), 166-72.

GLOVER, William L., and John O. Lenz. "A Cost Growth Model for Weapon System Development Programs." Master's thesis, Air Force Institute of Technology, School of Systems and Logistics, Wright-Patterson Air Force Base, Ohio, 1974.

GORDON, Harvey J. "The Role of the Contract in Systems Acquisition." Defense Systems Management Review, 3:1 (Winter 1980), 30-42.

Guide for Transitioning Army Missile Systems from Development to Production. Technical report RS-81-6. Army Missile Command, Redstone Arsenal, Ala.: Systems Engineering Directorate, July 1981.

HANRAHAN, John D. Government by Contract. New York: Norton, 1983.

HERSH, Michael H. "Risk Aversion vs. Technology Implementation." Student paper, Defense Systems Management College, Fort Belvoir, Va., 1977.

HLAVINKA, Duane K. "Lessons Learned: Production Restart of a Major Weapons System." Student paper, Defense Systems Management School, Fort Belvoir, Va., May 1976.

HOIVIK, Thomas Harry. "The Navy Test and Evaluation Process in Major Systems Acquisition." Student paper, Defense Systems Management College, Fort Belvoir, Va., 1976.

HOUSE, Robert J., and Steven Kerr. "Organizational Independence, Leader Behavior, and Managerial Practices." Journal of Applied Psychology, 58:2 (1973), 173-80.

HUNT, Raymond G. "Contractor Responses to Award Fee Contracts." National Contract Management Journal, 15:2 (Winter 1982), 84-90.

HWANG, John D., David Chappell, and Howard M. Gilby. "Risk Analysis of the Improved COBRA Armament Program." In Army Department (ed.), Proceedings, 12th Annual U.S. Army Operations Research Symposium, vol. 2, pp. 736-44. Washington, D.C.: 1973.

-----. "An Impact Assessment Algorithm for R&D Project Risk Analysis." Proceedings, 12th Annual U.S. Army Operations Research Symposium, October 2-5, 1973, vol. 2, pp. 559-71. Washington, D.C.: 1973.

INGALLS, Edward G., and Peter R. Schoeffel. "Risk Assessment for Defense Acquisition Management." In Robert F. Williams and Richard D. Abeyta (eds.), Management of Risk and Uncertainty in Systems Acquisition: Proceedings, pp. 55-64. Ft. Lee, Va.: Army Procurement Research Office, 1983.

-----. "Risk Assessment for Defense Acquisition Managers." Program Manager, September-October 1983, pp. 27-33.

INSLEY, Patricia A., et al. Shortening the Acquisition Cycle: Research on Concurrency (Phase I Report). Falls Church, Va.: Management Consulting and Research, 1982.

IRELAND, Lewis R. "A Risk Management Model for the Defense System Acquisition Process." In Robert F. Williams and Richard D. Abeyta (eds.), *Management of Risk and Uncertainty in Systems Acquisition: Proceedings*, pp. 192-99. Ft. Lee, Va.: Army Procurement Research Office, 1983.

JONES, Julius E. "An Analysis of Incentive Contracts with Respect to Risk." Master's thesis, Army Command and General Staff College, Fort Leavenworth, Kans., 1971.

KAUFMAN, Richard F. *The War Profiteers*. New York: Bobbs-Merrill, 1970.

KERNS, Waldon R., and Michael C. Tankersley. "Application of Risk Analysis: Response from a Systems Division." In Robert F. Williams and Richard D. Abeyta (eds.), *Management of Risk and Uncertainty in Systems Acquisition: Proceedings*, pp. 200-4. Ft. Lee, Va.: Army Procurement Research Office, 1983.

KIMPSTON, Richard D., and Leslie C. Sonnabend. "Public Secondary Schools: The Interrelationships Between Organizational Health and Innovativeness and Between Organizational Health and Staff Characteristics." *Urban Education*, 10:1 (April 1975), 27-45.

KOST, John D., Jr. *Defense Management Simulation (1973 Version)*. Washington, D.C.: Industrial College of the Armed Forces, Simulation and Computer Directorate, 1973.

LAVE, Lester R. (ed.). *Quantitative Risk Assessment in Regulation*. Washington, D.C.: The Brookings Institution, 1982.

LENK, Barry R. "Government Procurement Policy: A Survey of Strategies and Techniques." Student paper, George Washington University, Program in Logistics, Washington, D.C., 1977.

LEWARK, William H., Jr. "The Technical Assessment Annex—A Formal Technical Risk Analysis Role for the Air Force Laboratories in the DSARC Process." Student paper, Defense Systems Management School, Fort Belvoir, Va., 1975.

LEWIS, Warfield M., Jr. "A Simple Statistical Method of Presenting the Uncertainty Associated with Life Cycle Cost Estimates." Student paper, Defense Systems Management School, Fort Belvoir, Va., 1973.

LILGE, Ralph W. "Total Risk Assessing Cost Estimate (TRACE): An Evaluation." Army Aviation Research and Development Command, Systems and Cost Analysis Division, St. Louis, Mo., February 1979.

LOCHRY, Robert R., et al. Final Report of the USAF Academy Risk Analysis Study Team. Colorado Springs, Colo.: Air Force Academy, 1971.

LONG, John Amos. "Life Cycle Costing in a Dynamic Environment." Ph.D. diss., Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, 1983.

LONGSHORE, Douglas. "The Impact of the Emergency School Aid Act on Human Relations in Desegregated Elementary Schools." Educational Evaluation and Policy Analysis, 5:4 (Winter 1983), 415-24.

-----, Judith Kaye, and Vicki Mandel. Research on Human Relations. Santa Monica, Calif.: System Development Corp., 1981.

LORETTE, Richard J. "Do We Really Want Research on the Acquisition of Major Weapon Systems?" National Contract Management Journal, 10:2 (Winter 1976-77), 64-70.

LOSQUADRO, Joseph P. "Management Control in Weapons Systems Acquisition." Thesis, Naval Postgraduate School, Monterey, Calif., September 1978.

LOWRANCE, William W. Of Acceptable Risk: Science and the Determination of Safety. Los Altos, Calif.: William Kaufman, Inc., 1976.

MANN, Greg A. "VERT: A Risk Analysis Tool for Program Management." Defense Management Journal, 15:3 (1979), 32-36.

MCNICHOLS, Gerald R. "Cost-Risk Procedures for Weapon System Risk Analysis." Proceedings, Annual Reliability and Maintainability Symposium, Washington, D.C., January 27-29, 1981, pp. 86-94. New York: Institute of Electrical and Electronics Engineers, 1981.

MARTIN, Martin Dean. "A Conceptual Cost Model for Uncertainty Parameters Affecting Negotiated, Sole-Source Development Contracts." Ph.D. diss., University of Oklahoma, Norman, Okla., 1971.

MARTIN, Martin Dean, et al. "A Proposed Definition and Taxonomy for Procurement Research in the DOD." National Contract Management Journal, 11:2 (Winter 1977-78), 89-105.

-----. "An Evaluation of the Definition, Classification and Structure of Procurement Research in the DOD." National Contract Management Quarterly Journal, 12:4 (December 1978), 35-59.

MARTIN, M. D., Alan J. Rowe, and Herold A. Sherman (eds.). Management of Risk and Uncertainty in the Acquisition of Major Programs. Proceedings, Air Force Academy, Colorado Springs, Colo., February 9-11, 1981. Los Angeles, Calif.: University of Southern California, 1981.

MAZZA, Thomas N., and Robert C. Banash. "Decision Risk Analysis for XM204, 105mm Howitzer, Towed Reliability/Durability Requirements." In Army Department (ed.), Proceedings, 12th Annual U.S. Army Operations Research Symposium, vol. 2, pp. 445-60. Washington, D.C.: 1973.

MEEHAN, John D., and Thomas O. Millett. "Major Weapon System Acquisition: An Analysis of DOD Management Arrangements." Master's thesis, Air Force Institute of Technology, School of Engineering, Wright-Patterson Air Force Base, Ohio, September 1968.

MENEELY, Frank T. "Determining the Appropriate Contract Type." Concepts: The Journal of Defense Systems Acquisition Management, 5:3 (Summer 1982), 44-49.

MERIDIAN CORP. Preliminary Analysis of Technical Risk and Cost Uncertainty in Selected DARPA Programs. Falls Church, Va.: 1981. Includes interim and final reports.

MOORE, William F., and John M. Cozzolino. "More Effective Cost-Incentive Contracts Through Risk Reduction." Defense Management Journal, 14:4 (1978), 12-17.

MOREHOUSE, W. Progress in Resources Planning Through PERT. Utica, N.Y.: General Electric Co., Light Military Electronics Department, 1960.

MORROW, Garcia E., et al. Lessons Learned: Multiple Launch Rocket System. Arlington, Va.: Information Spectrum, 1980.

NAVY DEPARTMENT. "Justification of Estimates for Fiscal Year 1984." Document on weapons procurement submitted to the Congress, Washington, D.C., January 1983.

NEUMAN, Frederick. "How DCAA Uses Risk Analysis in Planning and Programming Audits." Internal Auditor, 36:3 (June 1979), 32-39.

NEUMAN, Gary. "Platoon Early Warning Device (PEWD) Decision Risk Analysis (DRA)." In Army Department (ed.), Proceedings, 12th Annual U.S. Army Operations Research Symposium, vol. 2, pp. 690-701. Washington, D.C.: 1973.

NIEMEYER, William A., et al. Technical Risk Assessment of Extended Configurations of the M113A1E1. Aberdeen Proving Ground, Md.: Army Materiel Systems Analysis Activity, 1978.

NORTON, Monte G., Richard D. Abeyta, and Paul E. Grover. Production Risk Assessing Methodology (PRAM). Fort Lee, Va.: Army Procurement Research Office, 1982.

O'FLAHERTY, J. Identification and Estimation of High Cost or High Risk Elements. McLean, Va.: Research Analysis Corp., 1970.

PACE, Dean Francis. Negotiation and Management of Defense Contracts. New York: Wiley-Interscience, 1970.

PALMER, Daniel L. "Evaluation of Automatic Transmissions for Use in Military Wheeled Vehicles (Decision Risk Analysis)." In Army Department (ed.), Proceedings, 12th Annual U.S. Army Operations Research Symposium, vol. 2, pp. 668-79. Washington, D.C.: 1973.

PEARCY, Stephan R. "Decision Analysis for XM578 APFSDS Cartridge Development Program." In Army Department (ed.), Proceedings, 12th Annual U.S. Army Operations Research Symposium, vol. 2, pp. 426-36. Washington, D.C.: 1973.

PERRY, Robert. American Styles of Military Research and Development. Santa Monica, Calif.: RAND Corp., 1979.

-----, et al. System Acquisition Strategies. Santa Monica, Calif.: RAND Corp., June 1971.

PETRUSCHELL, R. L. Project Cost Estimating. Santa Monica, Calif.: RAND Corp., September 1967.

RAIFFA, Howard. Decision Analysis: Introductory Lectures on Choices Under Uncertainty. Reading, Mass.: Addison-Wesley, 1968.

REID, Seton M. "Decision Risk Analysis of the AN/TSQ-73." In Army Department (ed.), Proceedings, 12th Annual U.S. Army Operations Research Symposium, vol. 2, pp. 718-24. Washington, D.C.: 1973.

RIPPY, D., and P. Sweeney. "Penetration Study: Behavioral Aspects of Decisions Under Uncertainty During Weapon System Acquisition." University of Dayton, School of Engineering, Dayton, Ohio, 1980.

ROWE, Alan J., and Ivan A. Somers. "History of Risk and Uncertainty Research in DOD." In Robert F. Williams and Richard D. Abeyta (eds.), Management of Risk and Uncertainty in Systems Acquisition: Proceedings, pp. 6-20. Ft. Lee, Va.: U.S. Army Procurement Research Office, 1983.

SCOTT, Eugene L. "The Cost Growth Phenomenon." National Contract Management Journal, 16:2 (Winter 1983), 37-45.

SHEA, Joseph F. "Observations on Defense Acquisition." Defense Systems Management Review, 1:4 (Autumn 1977), 29-36.

SHERRER, Charles W. "Achieving a Higher and More Competitive State-of-the-Art in DOD Procurement Procedures." National Contract Management Journal, 15:2 (Winter 1982), 71-83.

SIMONSON, G. R. "Misconceptions of Profit in Defense Policy." National Contract Management Journal, 15:2 (Winter 1982), 15-20.

SIZELOVE, J. Douglas. "Remotely Monitored Battlefield Sensor System (REMBASS) Program Decision Risk Analysis." In Army Department (ed.), Proceedings, 12th Annual U.S. Army Operations Research Symposium, vol. 2, pp. 712-17. Washington, D.C.: 1973.

SMITH, Charles H., and Charles M. Lowe, Jr. "Sole Source and Competitive Price Trends in Spare Parts Acquisition." National Contract Management Journal, 15:2 (Winter 1982), 51-56.

SMITH, Giles K. Air Force Acquisition Options for the 1980s: A Briefing on Study Plans. Santa Monica, Calif.: RAND Corp., 1979.

SOLINSKY, Kenneth S. "Controlled Competition for Optimal Acquisition." Defense Systems Management Review, 3:2 (Spring 1980), 47-55.

SPRINGER, Robert M., Jr. "Controlling Risk in Reliability Incentive Contracting." National Contract Management Journal, 9:2 (Winter 1975-76), 1-9.

STIMSON, Richard A., and A. Douglas Reeves. "Improving Defense Contractor Productivity." Defense Management Journal, 19:3 (1983), 41-44.

SUVER, James D., and F. Theodore Helmer. A Bibliography of Selected Studies in the Weapons Acquisition Area. Colorado Springs, Colo.: Air Force Academy, Department of Economics and Management, 1972.

SVETLICH, William G. The Systems Acquisition Process and Its Limitations in the Department of Defense. Washington, D.C.: National Defense University, 1979.

SWEENEY, Patrick J., and Douglas V. Rippy. "Behavioral Aspects of Decisions Under Uncertainty During Weapon Systems Acquisition." In M. D. Martin, Alan J. Rowe, and Herold A. Sherman (eds.), Management of Risk and Uncertainty in the Acquisition of Major Programs, pp. 76-78. Colorado Springs, Colo.: Air Force Academy, 1981.

THOMPSON, William E., III. "Risk Implications for Cost Growth in Weapon System Acquisition Programs." Concepts: The Journal of Defense Systems Acquisition Management, 5:2 (Spring 1982), 116-28.

TIMSON, F. S. Technical Uncertainty, Expected Contract Payoff, and Engineering Decisionmaking in a System Development Project. Santa Monica, Calif.: RAND Corp., 1970.

TRUEMAN, Richard E. An Introduction to Quantitative Methods for Decision Making. New York: Holt, Rinehart and Winston, 1974.

U.S. CONGRESS, House of Representatives. Improvements to the Department of Defense Acquisition Process Including Certificates of Competency. Hearings Before the Investigations Subcommittee of the Committee on Armed Services, 97th Cong., 1st sess. Washington, D.C.: U.S. Government Printing Office, 1983a.

U.S. CONGRESS, House of Representatives. Hearings Before the Committee on the Budget, 98th Cong., 1st sess. Washington, D.C.: U.S. Government Printing Office, 1983b.

-----. Hearings on H.R. 5167, Department of Defense Authorization of Appropriations for Fiscal Year 1985 and Oversight of Previously Authorized Programs, Before the Committee on Armed Services. Part 4. Research, Development, Test, and Evaluation—Title II, 98th Cong., 2nd sess. Washington, D.C.: U.S. Government Printing Office, 1984.

WALL, William C., Jr. "The Prudent Use of Engineers in Program Management." Defense Management Journal, 15:2 (1979), 14-18.

WELLISCH, Jean B., et al. "School Management and Organization in Successful Schools." Sociology of Education, 51 (July 1978), 211-26.

WENDT, Robert L. "Practical Implications of Acquisition Policy Reform." Defense Management Journal, 18:4 (1982), 15-19.

WENTZ, William. "Understanding How the Defense Department Allocates Resources." GAO Review, 49 (Summer 1983), 27-29.

WILLIAMS, Robert F., and Richard D. Abeyta (eds.). Management of Risk and Uncertainty in Systems Acquisition: Proceedings, Defense Risk and Uncertainty Workshop, Defense Systems Management College, Ft. Belvoir, Va., July 13-15, 1983. Fort Lee, Va.: Army Procurement Research Office, 1983.

WILLOUGHBY, Willis J., Jr. Best Practices for Transitioning from Development to Production. Chicago: Rand McNally, 1984.

WOO, John K. C. "Quantitative Risk Analysis of the Impact of Major Changes in Navy Programs." In Robert F. Williams and Richard D. Abeyta (eds.), Management of Risk and Uncertainty in Systems Acquisition: Proceedings, pp. 36-43. Ft. Lee, Va.: Army Procurement Research Office, 1983.

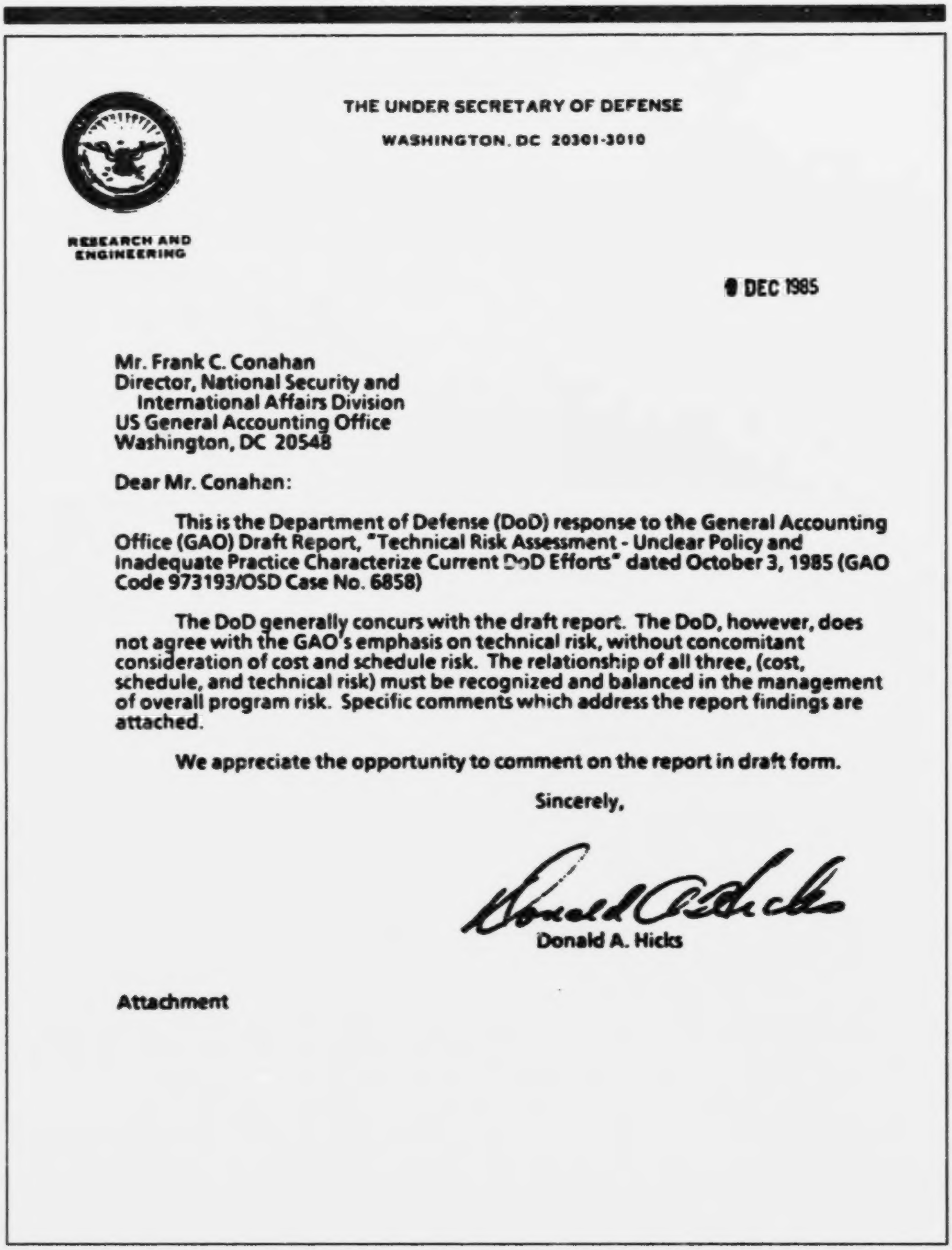
WOODY, James R. "DOD Procurement Policy: The Effect on Aerospace Financial Risk." Defense Management Journal, 18:3 (1982), 22-27.

WORM, George H. Application of Risk Analysis in the Acquisition of Major Weapon Systems. Clemson, S.C.: Clemson University, Department of Industrial Management, 1980.

Appendix III

Advance Comments from the U.S. Department of Defense

Note: GAO's response supplementing what is given in the report text appears at the end of this appendix.



THE UNDER SECRETARY OF DEFENSE
WASHINGTON, DC 20301-3010

RESEARCH AND
ENGINEERING

9 DEC 1985

Mr. Frank C. Conahan
Director, National Security and
International Affairs Division
US General Accounting Office
Washington, DC 20548

Dear Mr. Conahan:

This is the Department of Defense (DoD) response to the General Accounting Office (GAO) Draft Report, "Technical Risk Assessment - Unclear Policy and Inadequate Practice Characterize Current DoD Efforts" dated October 3, 1985 (GAO Code 973193/OSD Case No. 6858)

The DoD generally concurs with the draft report. The DoD, however, does not agree with the GAO's emphasis on technical risk, without concomitant consideration of cost and schedule risk. The relationship of all three, (cost, schedule, and technical risk) must be recognized and balanced in the management of overall program risk. Specific comments which address the report findings are attached.

We appreciate the opportunity to comment on the report in draft form.

Sincerely,

Donald A. Hicks

Donald A. Hicks

Attachment

GAO DRAFT REPORT DATED OCTOBER 3, 1985
(GAO CODE 973193) OSD CASE 6858

"TECHNICAL RISK ASSESSMENT: UNCLEAR POLICY AND INADEQUATE PRACTICE CHARACTERIZE CURRENT DOD EFFORTS"

DEPARTMENT OF DEFENSE COMMENTS

* * * * *

FINDINGS

o FINDING A: DoD Has Identified Technical Risks As A Factor Leading To Schedule Slippage and Cost Growth. The GAO observed that technical risks are inherent in the development of new weapon systems when performance requirements exceed the capabilities of current technology. According to GAO, if not anticipated and managed in the early phases of the acquisition process technical risks can have profound effects on program costs and schedules. GAO described technical risk assessments (TRA) as the process for identifying and evaluating the potential for performance problems, drawing a distinction between technological risk, and program risk, (which also includes schedule and cost risk). GAO reported that DoD has identified technical problems as a major factor in cost growth and schedule delay and has reported that the level of technical risk directly affects decisions on further development. The GAO further reported that it is the DoD postion TRA can significantly reduce the overall cost of acquiring new weapon systems. The GAO concluded that substantial savings could be expected from the design and implementation of TRAs. (pp. i, 1-1, p. 5-7/GAO Draft Report)

Now pp. 2, 10, and 77.

DoD Comments:

Partially concur. The DoD does not concur with the GAO report implication that technical risk should be emphasized in isolation. Technical risk is only one element of overall program risk, which also includes funding and cost risk, as well as schedule risk. It is essential that consideration of program risk include balanced consideration of each of the risk elements. The DoD does concur that early identification of technical risk, as well as other types of risk, should reduce program costs. It will also improve program stability and help ensure on-schedule contract performance. Since 1981, in fact, the DoD has been placing much greater emphasis on program risk, and has reduced cost growth to about one percent. It should be noted; however, that early identification of risk, while reducing the amount of cost growth, does not necessarily reduce program cost. It may simply cause recognition of additional cost initially thereby precluding it from being included in growth calculations.

o FINDING B: Despite Initiative 11, DoD Policies Regarding Technical Risk Assessment Remain Unfocused. The GAO found that Initiative 11 of DoD's 1981 Acquisition Improvement Program called for the use of quantitative technical risk assessments to support the budgeting of funds to cover risk. The GAO noted that many quantitative approaches are described in a handbook developed by the Defense Systems Management College (DSMC) in response to Initiative 11, and that other quantitative and qualitative tools are available. The GAO further noted that there are many resources available to aid Program Management Offices (PMOs) in performing technical risk assessments, but also observed that there are some obstacles to a clear understanding of DoD expectations. GAO pointed to no consistent definition of what is meant by technical risk as well as no DoD-wide definition of the commonly used terms high, medium, and low risk. While GAO acknowledged that some definitions exist for program risk, such as that developed by the DSMC and by Air Force Regulation 70-15, GAO nonetheless found no standard definition of technical risk in DoD. The GAO also observed that, while it is true that the regulations for documentation of major system acquisitions include requirements that technical risks be addressed, the degree of discussion or identification of risks is not set out, nor is there any specification of the kind of TRAs to be used. GAO found that there is no official policy or guidance calling for the application of specific tools or techniques, nor are there generic criteria for TRA, independent of the approach used. The GAO concluded that despite the fact Initiative 11 was intended to promote qualification of, and budgeting for, technical risks, in reality it has had little influence over the three Services' procedures for TRA. The GAO further concluded that there have been no perceptible changes in Defense Systems Acquisition Review Council (DSARC) procedures or operations as a result of Initiative 11. In summary, the GAO concluded that while the Department of Defense has general policies calling for TRA, the policies are unfocused and not clearly described under any regulation or directive. (pp. 2-1 through 2-17, and p. 5-2/GAO Draft Report)

Now pp. 3, 24-27, and 74.

DoD Comments:

Partially concur. The DoD concurs that policies relative to discrete treatment of technical risk remain unfocused, and that a generally accepted and understood definition of technical risk, including commonly used terms (high, medium, low risk), still does not exist within the DoD. As indicated in the response to Recommendation 1, the DoD will issue a handbook that incorporates DoD definitions of risk, including guidance on what constitutes high, medium and low risk, to the extent possible. DoD does not concur, however, that Initiative 11 has had little or no effect on the Services' or DSARC procedures for TRA. While it is difficult to identify specific actions attributable to Initiative 11, as noted in the response to Finding A, the overall program results are vastly improved.

o **FINDING C: Differences Among Program Offices In Addressing Technical Risk.** From its evaluation of 25 major-system Program management Offices (PMOs) for programs between Milestone I and III, GAO found that no PMOs quantified and budgeted for technical risks, as called for by Initiative 11. Lacking DoD criteria for what constituted a TRA, the GAO developed criteria for minimal standards of quality for TRAs, stating that risk efforts (REs) should be:

- prospective, examining risks before problems occurred;
- planned, not an incidental part of program discussions;
- explicit in attention to technical risks;
- documented, so that the results of the assessment could be shared with decision-makers and staff; and
- reported twice in each acquisition phase to determine how risks were changing.

The GAO reported, that although all 25 PMOs made an effort to identify their technical risks, only three conducted risk efforts meeting the GAO-developed criteria for TRAs. In addition, the GAO observed wide variation in how risk efforts are implemented. Although formats for assessing risk are generally most useful when they combine a description of technical problems with qualitative or quantative rating--i.e., when they specify the content and level of risk, GAO found that few PMOs used such formats. The GAO also noted that risk efforts are generally most informative when they cover all subsystems, not just selected ones or the system as a whole, yet few PMOs did so. The GAO also noted that reliability of risk input is enhanced when several raters provide written input independently, but again, few PMOs followed that procedure. The GAO also concluded that inasmuch as most PMOs did not consider the complexity or maturity of their systems when choosing implementation options, it was not likely that their risk efforts, as implemented, were as useful as they could have been in furthering system development. (pp. 3-1 through 3-31, GAO Draft Report)

Now pp. 3, 34-48,
and 74-75.

DoD Comments:

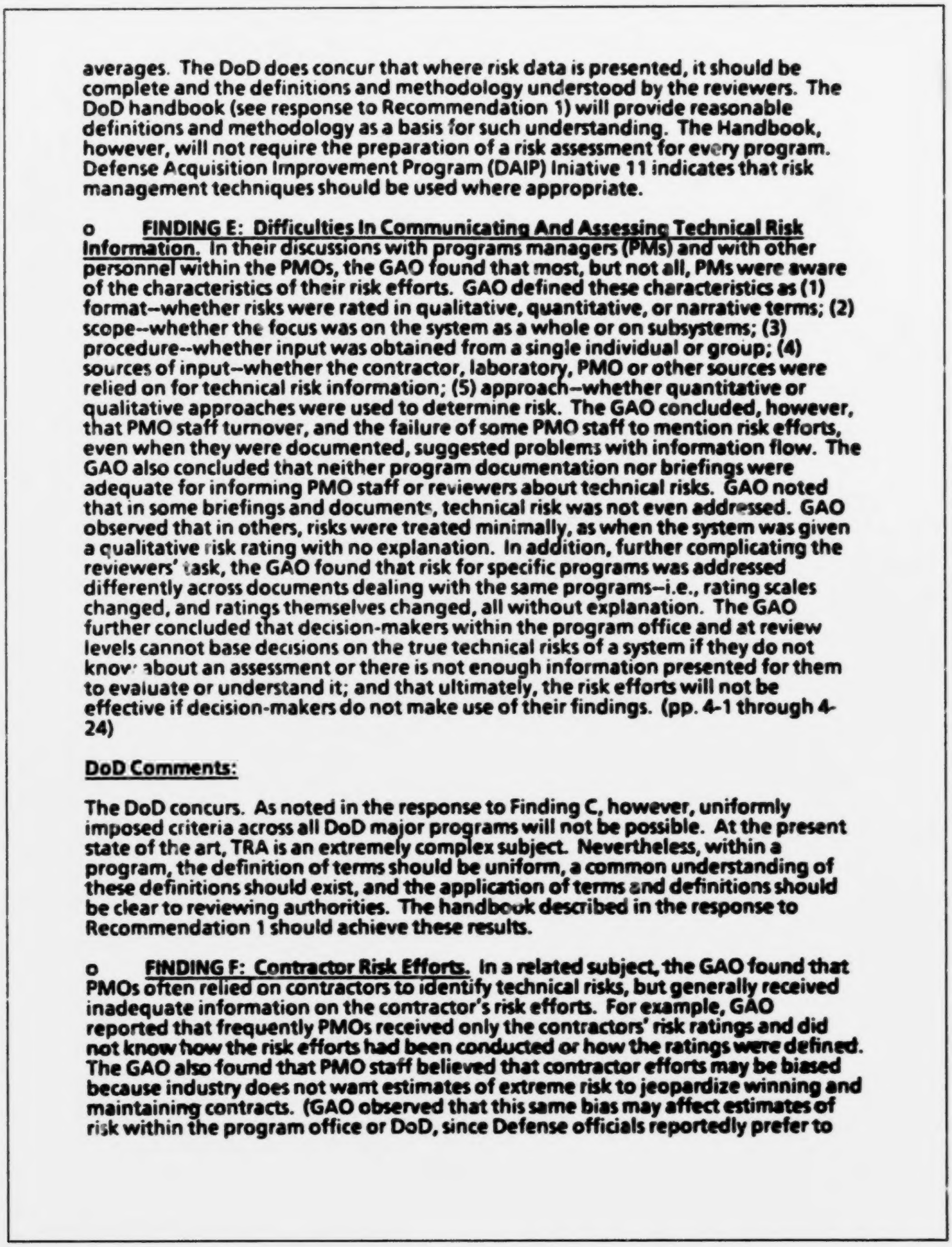
Partially concur. The DoD does not concur that risk efforts were less useful than they could have been in furthering system development. As GAO pointed out (since it did not assess the actual experience or degree of success of the systems studied), it could not determine whether TRAs actually chosen for each program were the most appropriate. The DoD does concur that there should be criteria for TRA in generalized form, with allowances for tailoring to specific program circumstances. It will not be possible, however, to measure all TRA efforts against uniformly imposed criteria. Each major system is unique in a number of respects. The success of one system may be dependant upon the development of new technologies, while another system may employ only proven technologies. Thus, the description of risks as high, medium or low must be measured on a relative scale, rather than on any absolute scale. TRA is comprised of a number of analytical tools which should be carefully selected and tailored to the specific circumstances present on a particular system. Prescribing a standard methodology to be strictly applied across a broad spectrum of individual program circumstances would be extremely difficult, and the desirability of doing so would certainly be open to question. The selection of TRA areas within a program must generally be left to the Program/Project Manager, the individual most familiar with the program risks.

o **FINDING D: Information Provided For Service And DSARC Review.** The GAO observed that (in order to be useful) decisions regarding the pace and direction of these programs must be made during milestone reviews at the Service and at DSARC levels. The GAO found, however, that, on the average, technical risk information was presented in only 80 percent of the various documents for Milestone I and in 76 percent for Milestone II. The GAO further found that the analytical approach used and the scope of risk was almost never reported in these documents. After reviewing briefing charts, minutes and scripts used in these reviews, GAO concluded that it was unlikely that much information was conveyed orally to reviewers on the approach and scope of the risk effort. The GAO also concluded that milestone decision documents rarely combined narrative information with qualitative or quantative ratings for all subsystems. (pp. 3-1 through 3-31, pp. 5-3, through 5-7/GAO Draft Report)

Now pp. 4, 48-51,
and 75.

DoD Comments:

Partially concur. The DoD does not concur with GAO's methodology for arriving at 80 and 76 percent, respectively. The DoD guidance does not require a risk assessment in several of the documents which the GAO used in calculating these



averages. The DoD does concur that where risk data is presented, it should be complete and the definitions and methodology understood by the reviewers. The DoD handbook (see response to Recommendation 1) will provide reasonable definitions and methodology as a basis for such understanding. The Handbook, however, will not require the preparation of a risk assessment for every program. Defense Acquisition Improvement Program (DAIP) Iniative 11 indicates that risk management techniques should be used where appropriate.

o **FINDING E: Difficulties In Communicating And Assessing Technical Risk Information.** In their discussions with programs managers (PMs) and with other personnel within the PMOs, the GAO found that most, but not all, PMs were aware of the characteristics of their risk efforts. GAO defined these characteristics as (1) format--whether risks were rated in qualitative, quantitative, or narrative terms; (2) scope--whether the focus was on the system as a whole or on subsystems; (3) procedure--whether input was obtained from a single individual or group; (4) sources of input--whether the contractor, laboratory, PMO or other sources were relied on for technical risk information; (5) approach--whether quantitative or qualitative approaches were used to determine risk. The GAO concluded, however, that PMO staff turnover, and the failure of some PMO staff to mention risk efforts, even when they were documented, suggested problems with information flow. The GAO also concluded that neither program documentation nor briefings were adequate for informing PMO staff or reviewers about technical risks. GAO noted that in some briefings and documents, technical risk was not even addressed. GAO observed that in others, risks were treated minimally, as when the system was given a qualitative risk rating with no explanation. In addition, further complicating the reviewers' task, the GAO found that risk for specific programs was addressed differently across documents dealing with the same programs--i.e., rating scales changed, and ratings themselves changed, all without explanation. The GAO further concluded that decision-makers within the program office and at review levels cannot base decisions on the true technical risks of a system if they do not know about an assessment or there is not enough information presented for them to evaluate or understand it; and that ultimately, the risk efforts will not be effective if decision-makers do not make use of their findings. (pp. 4-1 through 4-24)

Now pp. 3, 62-67, and 76.

DoD Comments:

The DoD concurs. As noted in the response to Finding C, however, uniformly imposed criteria across all DoD major programs will not be possible. At the present state of the art, TRA is an extremely complex subject. Nevertheless, within a program, the definition of terms should be uniform, a common understanding of these definitions should exist, and the application of terms and definitions should be clear to reviewing authorities. The handbook described in the response to Recommendation 1 should achieve these results.

o **FINDING F: Contractor Risk Efforts.** In a related subject, the GAO found that PMOs often relied on contractors to identify technical risks, but generally received inadequate information on the contractor's risk efforts. For example, GAO reported that frequently PMOs received only the contractors' risk ratings and did not know how the risk efforts had been conducted or how the ratings were defined. The GAO also found that PMO staff believed that contractor efforts may be biased because industry does not want estimates of extreme risk to jeopardize winning and maintaining contracts. (GAO observed that this same bias may affect estimates of risk within the program office or DoD, since Defense officials reportedly prefer to

Now pp. 5, 69-71, and 76.

fund systems with low to moderate technical risk.) The GAO concluded that PMOs did not receive sufficient information, in most instances, to evaluate the adequacy or accuracy of the contractors' risk efforts. (p. iii, 4-2, through 4-31, 5-5, and 5-6, GAO Draft Report)

DoD Comments:

The DoD concurs. In those cases where TRA is conducted by the contractor, the information presented should be sufficient for a complete understanding of methodology, definition of terms, etc. used by the contractor in the analysis

Now pp. 4, 67-69, 71, and 76.

o **FINDING G: Staffing And Training For Program Office Risk Efforts.** The GAO reported that, in the majority of PMOs, the staffs were involved in both selecting and performing the risk efforts. Despite this, however, GAO found that technical risk assessment receives little attention in the Services' training courses. The GAO found that the Army is the only Service with a course on risk as part of its regular course offerings. The GAO further found that when risk is mentioned, it is broadly defined as "program risk," and technical risk is addressed only minimally and that neither the Service schools, nor the DSMC, discuss approaches for assessing technical risk. The GAO concluded that, generally, there appears to be insufficient training available to support the performance of TRAs. (p. iii, pp. 4-24 through 4-28, p. 4-31, p. 5-5/GAO Draft Report)

DoD Comments:

Partially concur. The DoD does not agree that the information in the GAO report, or other data available to the DoD, supports a conclusion that there is insufficient training to support the performance of TRAs. For instance, the DSMC provides the following coverage of risk:

a. Program Management Course 85-2;
Instructional Unit T2.1130-1140 Risk Management

b. Program Management Course 86-1;
Instructional Unit T2.1130-1140 Risk Management New Unit: Risk Workshop - a six hour workshop utilizing personal computer sized model to evaluate changes and provide the student with an understanding of risk management.
New Unit; Quantifative Methods for Program Planning and Control - a problem oriented unit to illustrate how the PM can integrate performance, schuedule, cost, risk & uncertainty.

c. Program Managers Workshop:
A Risk Management Workshop has been a regular part of this course since its inception in January 1984.

d. 1983 Defense Risk and Uncertainty Workshop:
USA Sponsored/DSMC Hosted; 13-15 July 1983.

e. Risk Assessment Techniques - A Handbook for Program Management Personnel: First Edition; July 1983.
Developed and published by DSMC.

f. System Engineering Management Guide: First Edition; October 1983

(Second Edition currently underway). Developed and published by DSMC. Chapter 22 is entitled: Risk Analysis and Management.

g. Computer Models are currently in use or in development by DSMC as follows:
   1. DPESO Model
   2. TRACE Model
   3. CASA Model

All of the above models are being sized to run on the DSMC Personal Computers.

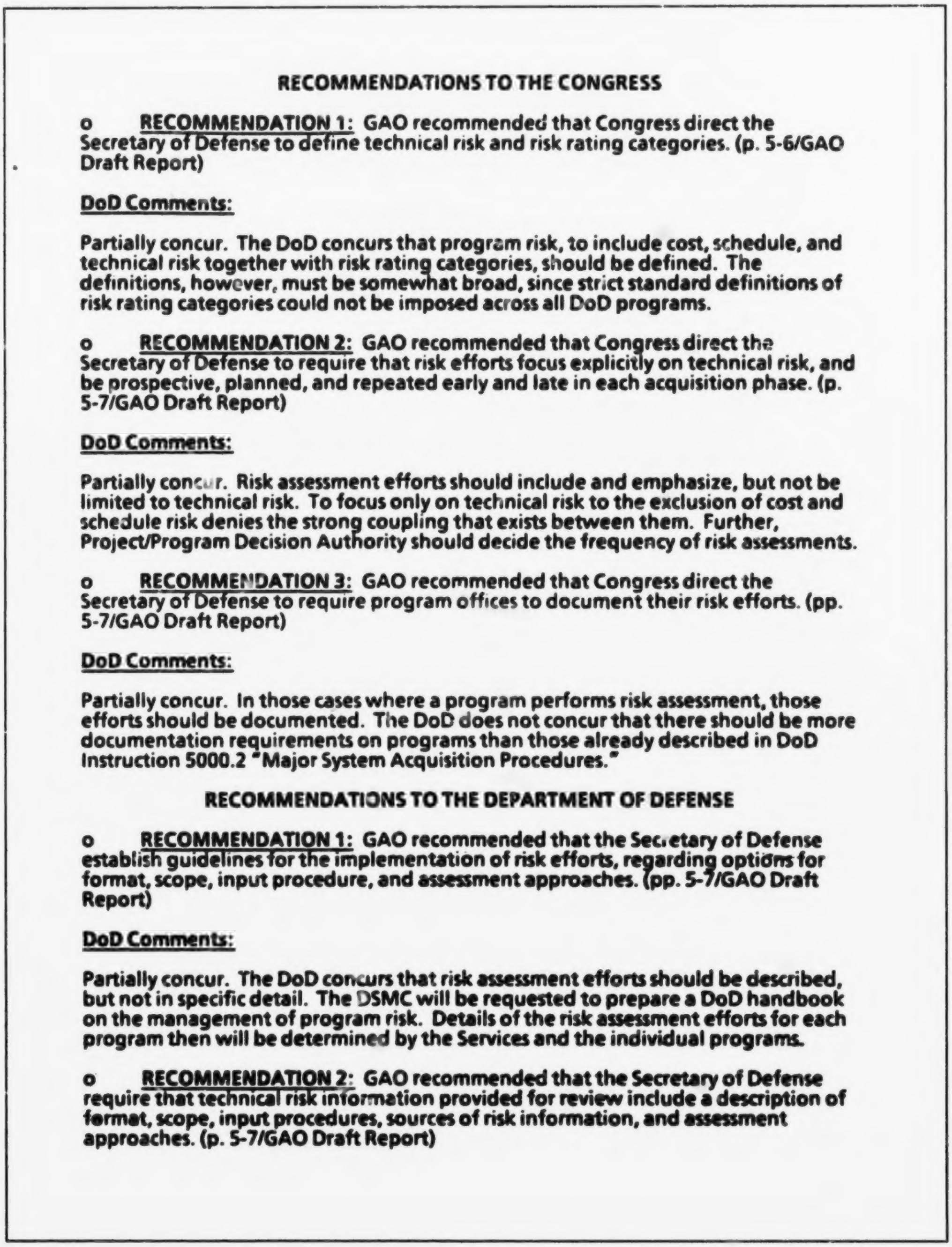
The DoD concurs that technical risk is taught in the context of program risk. The DoD agrees also that technical risk assessment, in the context of overall program risk, will be given increased emphasis. The DoD handbook being developed (see response to Recommendation 1) will help in this effort.

o **FINDING H: Definitions Of Risk and Risk Rating Categories.** The GAO found that few PMOs know how the Services or DoD documents define risk. For example, GAO reported that no PMO cited the DSMC definition, and only one Air Force PMO was aware of the definition of risk in Air Force Regulation 70-15. The GAO found that while many PMOs had a definition of risk shared by most staff members, the definitions varied widely across PMOs. GAO reported that many PMOs expressed risk in qualitative ratings--high, moderate, low, or red, yellow, green. Their ratings were, in turn, defined in narrative or quantitative terms. For example, high risk was sometimes defined narratively as, "beyond the state of the art," or defined quantitatively, as at least an 80 percent chance of failure. The GAO concluded that narrative as well as quantitative definitions were widely divergent across all PMOs and were often contradictory. The GAO further concluded that with definitions and ratings so inconsistent, confusion is almost inevitable. In addition, the GAO concluded that the results of any risk effort performed without regard for such inconsistencies will not be very valuable and may mislead decision-makers. Finally, the GAO concluded that the PMOs' current approach to addressing technical risk offers no guarantee that requisite information will be provided to decision-makers inside the PMO or at the higher levels of review. (pp. 4-1, p. 4-16, p. 4-31, pp. 5-5/GAO Draft Report)

Now pp. 3, 54-62, 71, and 76.

DoD Comments:

Partially concur. The DoD concurs that definitions of risk should be consistent, and that these definitions should be understood by program personnel as well as by the decision makers reviewing the program. As indicated above, a DoD handbook will address these. The DoD does not concur, however, with the implication that standard definitions will set out a uniformly applicable categorization of risk, which will necessarily provide comparability from program to program. Considering the diversity of risks encountered across a broad spectrum of programs, each with unique problems, selection of risk assessment tools, methodology and risk definitions should be tailored to best suit the individual program. Once defined, they must be uniformly understood. Risk assessment should not be considered as an exact science, but should be recognized as the art that it is at the present time.



RECOMMENDATIONS TO THE CONGRESS

Now p. 77.

o **RECOMMENDATION 1:** GAO recommended that Congress direct the Secretary of Defense to define technical risk and risk rating categories. (p. 5-6/GAO Draft Report)

DoD Comments:

Partially concur. The DoD concurs that program risk, to include cost, schedule, and technical risk together with risk rating categories, should be defined. The definitions, however, must be somewhat broad, since strict standard definitions of risk rating categories could not be imposed across all DoD programs.

Now p. 77.

o **RECOMMENDATION 2:** GAO recommended that Congress direct the Secretary of Defense to require that risk efforts focus explicitly on technical risk, and be prospective, planned, and repeated early and late in each acquisition phase. (p. 5-7/GAO Draft Report)

DoD Comments:

Partially concur. Risk assessment efforts should include and emphasize, but not be limited to technical risk. To focus only on technical risk to the exclusion of cost and schedule risk denies the strong coupling that exists between them. Further, Project/Program Decision Authority should decide the frequency of risk assessments.

Now p. 77.

o **RECOMMENDATION 3:** GAO recommended that Congress direct the Secretary of Defense to require program offices to document their risk efforts. (pp. 5-7/GAO Draft Report)

DoD Comments:

Partially concur. In those cases where a program performs risk assessment, those efforts should be documented. The DoD does not concur that there should be more documentation requirements on programs than those already described in DoD Instruction 5000.2 "Major System Acquisition Procedures."

RECOMMENDATIONS TO THE DEPARTMENT OF DEFENSE

Now recommendation 4 on p. 77.

o **RECOMMENDATION 1:** GAO recommended that the Secretary of Defense establish guidelines for the implementation of risk efforts, regarding options for format, scope, input procedure, and assessment approaches. (pp. 5-7/GAO Draft Report)

DoD Comments:

Partially concur. The DoD concurs that risk assessment efforts should be described, but not in specific detail. The DSMC will be requested to prepare a DoD handbook on the management of program risk. Details of the risk assessment efforts for each program then will be determined by the Services and the individual programs.

Now recommendation 5 on p. 77.

o **RECOMMENDATION 2:** GAO recommended that the Secretary of Defense require that technical risk information provided for review include a description of format, scope, input procedures, sources of risk information, and assessment approaches. (p. 5-7/GAO Draft Report)

DoD Comments:

Non-concur. It is not necessary for the Secretary of Defense to require explicit elements of risk review information and assessment approaches. Technical risk of a specific system may be well understood by DSARC members, or may require varying degress of elaboration in documents presented during reviews. DoD Instruction 5000.2 provides for the submittal of data as determined by the Defense Acquisition Executive, and requests for data result from a review of program documentation by various staff elements of the Office of the Secretary of Defense prior to DSARC milestones. This data, together with the guidance in the new DoD handbook, should provide the basis for full understanding of other risk elements involved in individual program reviews.

Now recommendation 6 on p. 77.

- **RECOMMENDATION 3:** GAO recommended that the Secretary of Defense should consider providing additional, more focused training in technical risk assessments to support a greater emphasis on technical risks. (pp. 5-8/GAO Draft Report)

DoD Comments:

Partially concur. The DoD concurs that risk should be emphasized. Greater emphasis on risk assessment techniques is ongoing in the context of overall program risk. However, emphasis should not be focused just on technical risk assessments, which is only a part of program risk. The emphasis must be a balanced approach to the management of program risk. (Also see response to Finding G.)

Now recommendation 5 on p. 77.

- **RECOMMENDATION 4:** GAO recommended that the Secretary of Defense require contractor risk efforts to be sufficiently documented to allow independent evaluation and use in the program office. (pp. 5-8/GAO Draft Report)

DoD Comments:

Concur. Where contractors perform the risk analysis, this effort should be sufficiently documented. Concurrence does not imply, however, that all programs must have contractors perform risk assessment as a part of their contract. When required and included in the contract, the program must provide appropriate contractual language and direction to guide contractor's efforts and insure a satisfactory product. Specific guidance in this area also will be covered in the new DoD handbook.

Following is our response to comments from the U.S. Department of Defense in its December 9, 1985, letter.

GAO's Response

"Finding A"

As requested by the Senate Governmental Affairs Committee, the subject of this report is technical risk. This does not mean that we support an approach to program management that de-emphasizes cost or schedule risk. On the contrary, it is precisely the relationship between technical risk, on the one hand, and cost and schedule problems, on the other, that prompted GAO's review. If one considers technical risk as the independent variable and cost and schedule problems as dependent variables—on this point, we agree with DOD—then the proper treatment of technical risk covers cost and schedule risk to some degree. Nevertheless, in this report we have explicitly considered cost and schedule risks. Our review of the phases of acquisition in chapter 1 refers to a wide range of considerations affecting development—cost and schedule problems as well as technical ones. In chapter 2, we noted that cost, schedule, and technical problems are interdependent. Thus, we have focused on technical risk but have not isolated it from other important risk elements. In response to DOD's comment, we revised these chapters in order to emphasize the importance of cost and schedule problems as well as technical ones.

However, we found some DOD assessments that measured cost or schedule risk without differentiating the sources of these risks as technical or other kinds of problems. Moreover, risk assessors are sometimes asked to estimate the likelihood of encountering technical problems given specific cost or schedule constraints; hence, we have emphasized that assessments should expressly identify technical as well as cost and schedule problems. What is clearly needed is a balance of attention to technical, cost, and schedule risks.

DOD states that early risk assessments can reduce cost growth but do not necessarily reduce program cost. Actually, either outcome is beneficial. But reduced program cost is certainly more likely if risks are identified and monitored carefully from the outset.

"Finding B"

DOD claims that Initiative 11 reduced cost growth, but as we reported in chapters 2 and 3, none of the 25 program management offices has performed a quantitative technical risk assessment for use in budgeting, and Initiative 11 has not stimulated new policy in the services or the DSARC regarding the identification and quantification of technical risks. DOD has not disputed these findings. It is reasonable to conclude that the reported reduction in cost growth stems from other factors, such as the reduced inflation rates in recent years.

"Finding C"

Neither the current nor the eventual success of these programs is the only basis for determining whether risk assessment procedures are adequate. Principles derived from experience also offer valuable guidance. Presumably working from previous experience, DOD approves of assessment criteria "in generalized form" but would reserve decisions on "analytical tools" for program managers. These comments are consistent with the conclusions we drew from our analysis of program management experience inside and outside DOD. The five criteria we have set out are generic—that is, they are appropriate for all major programs. With respect to analytical approaches and implementation, we have recognized the need for flexibility, since decisions in analysis and implementation depend on particular characteristics of systems such as their maturity and complexity. Few of the program offices have performed technical risk assessments meeting the five criteria, and few considered the maturity and complexity of their systems when conducting their assessments. Thus, despite the absence of data on the effects of risk assessments, it remains unlikely that most of the assessments we found were as useful to program managers and reviewers as they might have been.

We have recommended that rating categories such as high, medium, and low be defined, but we thought that the development of definitions should be left to DOD. DOD's forthcoming handbook will apparently provide definitions of technical risk and of risk rating categories (see DOD's comments under "Finding B"). However, we reiterate our statements in chapter 4 on the need for definitions that can be applied across programs in order to reduce existing disparities in basic risk concepts and, thereby, facilitate management and review. The task is to find as much common conceptual ground as possible between programs or meaningful subsets (for example, high-technology programs). We have reported that the Air Force took this approach in defining program risk in Air Force Regulation 70-15. It is difficult to imagine a handbook for general use that would not attempt to find this common ground.

"Finding D"

We have pointed out in chapters 2 and 3 that DOD regulations require coverage of technical risk in the milestone documents. DOD Instruction 5000.2 and the Army's Materiel Acquisition Handbook (DARCOM-P 70-2) call for information on risk areas and risk reduction efforts in the system concept paper, decision coordinating paper, integrated program summary, and acquisition strategy. DOD Instruction 5000.3 requires discussion of critical issues in the test and evaluation master plan, specifically including issues arising from technical risk. This coverage is not possible without some sort of risk assessment, however formal or informal, extensive or brief. We searched for technical risk information in these documents, whether or not it was explicitly linked to any assessment, but found no such information in 20 to 24 percent of the documents. It is important that technical risk information always be available in program reviews and that this information cover both the methods and the results of an assessment. Reviewers can then evaluate the information and weigh it, as they choose, along with other factors considered at each milestone.

"Finding E"

We recognize that technical risk assessment is complex and must take particular program circumstances into account. But modern, "high tech" weapon systems are also complex, and there is really no alternative to a careful, thorough assessment of the technical risks involved in developing these systems. As we have noted in our response to DOD's comment under "Finding C," generic criteria for risk assessment can be developed and applied without sacrificing flexibility. We have further noted that it is important that definitions of technical risk and of rating categories, in the manner of Air Force Regulation 70-15, be general enough for use across programs. We hope that the forthcoming DOD handbook will accommodate these purposes.

"Finding F"

No response is necessary.

"Finding G"

The conclusions cited under "Finding G" are based on an analysis of the courses, workshops, and handbooks DOD refers to. The courses and workshops either cover technical risk minimally or do not mention it at all. Other resources describe assessment techniques but provide no guidance for selecting techniques that are suitable for particular programs. It is important to note that most of the courses and workshops cited in DOD's comments cover risk management, not risk assessment. As we have noted in chapter 2, risk management deals with problems as they arise, whereas risk assessment identifies problems in advance. Thus, risk assessment alerts program staff members to problems that they try to avoid or solve through subsequent risk management. DOD's courses do not provide enough coverage of the concepts and analytical tools that are used in the assessment of specifically technical risks. Several of our other findings, such as the inconsistency in definitions of risk and risk rating categories and the lack of explicit attention to technical risk, are further evidence of the inadequacy of current training. In short, the technical content of DOD's training for risk assessment lags behind the technical content of the weapon systems being developed.

"Finding H"

DOD has misconstrued our conclusions under "Finding H." We have not called for a standard set of concepts and tools to be applicable in all respects to every program. We have noted in chapter 3 that technical risk assessment requires some decisions that cannot be considered generic. Various concepts and tools in technical risk assessment are, moreover, not uniformly appropriate for all programs (as we also note in chapters 2 and 4). But much of the potential advantage of technical risk assessment is lost if managers and reviewers cannot compare assessment procedures and results in general terms across at least some programs, such as those that use similar technologies. Comparability across programs facilitates an analysis of the trade-offs between two or more systems competing for further funding. It also helps reviewers formulate and follow up on their own concerns regarding systems with similar technical features. And, finally, comparability across programs reduces the time it takes to become familiar with any one system under review; decisionmakers do not have to learn a new language of risk (concepts, procedures, results) for each system they examine. We reiterate our response to DOD's comments under "Finding C": the task is to find the common ground in defining and assessing technical risk, as Air Force Regulation 70-15 does in its definition of program risk.

Recommendation 1

In the draft that DOD reviewed, we made three recommendations to the Congress and four to the secretary of Defense. For the final draft, we directed all the recommendations to the secretary, subsuming the topic of contractors' risk efforts (originally recommendation 4 to the secretary) under what is now recommendation 5. The content of all the recommendations is the same in the published report as in the draft DOD reviewed.

Cognizant of differences across DOD programs, we support guidelines that are as precise as possible and as flexible as necessary. The development of such guidelines may not be easy, but it is nonetheless critical to effective program management and review. Since it is often necessary to estimate the likelihood of technical problems under specific cost or schedule constraints, definitions and procedures should be devised for each component of program risk, not just for program risk in general. If an estimate of technical risk is required, analysts can use those definitions and procedures to provide it.

Recommendation 2

We have called for explicit attention to technical risk, not for exclusive attention. Technical problems should be described and evaluated clearly, not left implicit in assessments of cost or schedule risk. As we have stated in the report, we support risk assessment at least twice—early and late—in each acquisition phase, to inform decisionmakers regarding work in that phase and progress to the next. But technical risks are ongoing and, as DOD believes, decisions regarding the frequency and type of assessment are best left to program managers. The wording of this recommendation was changed in the final draft in order to clarify our position: the recommendation for two assessments in each phase now calls for at least two assessments in each phase.

Recommendation 3

The purpose of documentation is to make it possible to track risks throughout the acquisition cycle. Only if records are kept can reviewers and program staff fully understand, evaluate, and update past assessments. The records need not be lengthy, so long as they adequately describe assessment procedures and results.

Recommendation 4

We hope that DOD's forthcoming handbook will be detailed enough to provide useful guidance regarding format, scope, data collection, and assessment approaches. We have reported that we found a wide variety of risk concepts and procedures among the 25 program offices in the study. We also found general inattention to the complexity and maturity of systems as assessment options were selected. For these reasons, it is important that DOD not merely enumerate various risk concepts and procedural options but also formulate advice for selecting appropriate concepts and options.

Recommendation 5

DOD already requires risk information in program reviews, but the information now provided is inadequate in several respects. We have characterized the kind of information that would provide an adequate basis for understanding and evaluating risk assessment procedures and that would therefore be appropriate for inclusion in review documents. For some programs, reviewers may already know the technical risks or may decide that they do not need all the information we would make available. But it is important that the information be available for every reviewer who wishes to see it. (This position underscores the need for documenting assessments. Without a written record, information requested later by reviewers may not be retrievable.)

Recommendation 6

We believe that attention to technical risk should be explicit rather than being left implicit in cost or schedule risk assessments. We agree that cost and schedule risks also require careful attention. But in our review, we found serious inadequacies in DOD's current training for technical risk assessment. Courses, handbooks, and other training resources may require formal revision to ensure full and proper attention to risks that are distinctly technical.

Further, as we have noted in our response to DOD's comment under "Finding G," it is important to distinguish risk assessment from risk management. DOD's training stresses risk management. Hence, we propose that training emphasize not just technical risk but also assessment, as distinct from management.

Recommendation 4 (Now in Recommendation 5)

We have not proposed that technical risk assessments be required of all contractors. But when a contract or request for proposal does make the requirement, specific information is essential—the same information we have recommended for program offices' documentation of risk. The information covers format and scope of the risk ratings, information sources, data collection, and the analytic approach.

Requests for copies of GAO reports should be sent to:

U.S. General Accounting Office
Post Office Box 6015
Gaithersburg, Maryland 20877

Telephone 202-275-6241

The first five copies of each report are free. Additional copies are $2.00 each.

There is a 25% discount on orders for 100 or more copies mailed to a single address.

Orders must be prepaid by cash or by check or money order made out to the Superintendent of Documents.

128